Select a country

← Technical Studio Home

Configuring the OS/400 LDAP Server

· Verify these Pre-Configuration Tasks

· Configure and start the OS/400 LDAP server

· Publish to the LDAP directory from the OS/400 SDD

· Verify the connection to the OS/400 LDAP server

Download PDF version 1.2Mb

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

Configure the OS/400 LDAP Server
*Updated: Oct, 19 2001*
Covers: OS/400 V5R1

Right-Click to download an Adobe PDF file of this topic.(1.2Mb)

Single sign on (SSO) is becoming a requirement when users want to access both iSeries and Domino data from a single Web browser. Web browsers can authenticate once to a Domino server or a Websphere server, then access any other Domino or Websphere servers in the same DNS domain that are enabled for SSO without signing on again.

An LDAP (Lightweight Directory Access Protocol) directory is required to implement Single Sign-On between Domino and Websphere servers.

This workshop will lead you through the steps required to configure your OS/400 for LDAP directory services. This includes publishing the System Distribution Directory (SDD) to the LDAP directory. The SDD stores information about all of the users who subscribe to your internal e-mail system. (For an explanation of adding users to the SDD check out *e-business 101* lesson 3, step 2.)
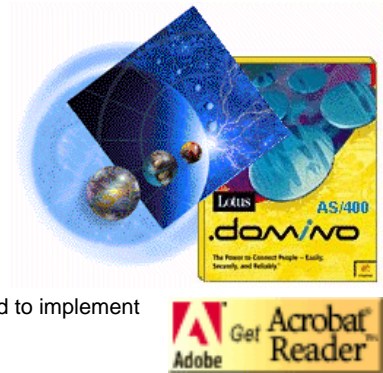
> **Note:** This workshop is part of a 2001 ITSO Forum presentation and lab "*Domino and Websphere Integration on iSeries*": Presentation pdf (909kb) ; Full Domino Websphere Integration Lab .PDF file (2.6MB) ; Presentation Freelance .PRZ file (2.45MB).
>
> All current Forum materials can be found at:
> http://www.ibm.com/services/learning/community/as400/itso/

To configure LDAP on your iSeries or AS/400 server:

1. Verify these pre-configuration tasks.
2. Configure and start the OS/400 LDAP server.
3. Publish to the LDAP directory from the OS/400 SDD.
4. Verify the connection to the OS/400 LDAP server.

Completing these steps configures your iSeries server as an LDAP server.

Verify these prerequisites for OS/400 LDAP
In this workshop, you'll configure your OS/400 for LDAP.

Before continuing with this workshop, make sure that:

1. Your OS/400 is **V4R3 or higher** and the updated PTF's and fixes are installed.

2. **Prior to V4R5**: you verify that **Directory Services** has been installed in your OS/400. (This is included free with OS/400; Option number 32 of 5769-SS1.)
   a. From an iSeries Command prompt, type:

      DSPSFWRSC
   b. Press the **Enter** key. The *Display Software Resources* screen appears:
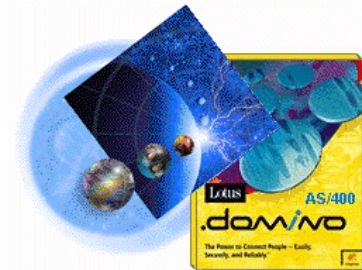
```
                                      Display Software Resources

Resource
   ID       Option   Feature    Description
5769SS1     32       5050       OS/400 - Directory Services
5769SS1     32       2924       OS/400 - Directory Services
5769SS1     33       5111       OS/400 - Private Address Sp
5769SS1     34       5050       OS/400 - Digital Certifica
5769SS1     34       2924       OS/400 - Digital Certific
5769SS1     35       5050       OS/400 - Cryptographic S
5769SS1     35       2924       OS/400 - Cryptographic S
5769SS1     36       5112       OS/400 - PSF/400 1-20 IP
5769SS1     37       5113       OS/400 - PSF/400 1-45 IP
5769SS1     38       5114       OS/400 - PSF/400 Any Sp
5700NT1     *BASE    5050       Native Tools (NATT) -
5700NT1     *BASE    2924       Native Tools (NATT)
5700NT1     1        5051       NATT QDEVELOP Libra
5700NT1     1        2924       NATT QDEVELOP Libra

Press Enter to continue.

F3=Exit    F11=Display libraries/releases
F19=Display trademarks
```

Page down and look for option number **32** of **5769-SS1**.

> **Note:** In OS/400 V5R1 or later, Directory Services is part of the base operating system.

3. You have installed and configured (on your PC) **Client Access Operations Navigator**. For more information about Operations Navigator, visit the Web sites at *Technical Studio* for V4R4 and the *Information Center* for V4R5 or V5R1.

> **Note:** All directory server configuration tasks are performed using Operations Navigator.

4. You verify that you know the password of an OS/400 user profile with *ALLOBJ and *IOSYSCFG special authorities.
   To display a user profile:

   a. From an iSeries Command prompt, type:

      DSPUSRPRF *username*

      where *username* is the user ID you will use for configuration tasks.
   b. Press **F4**. Use Option **5** to display the user's settings.

5. You plan ahead and define a suffix or naming context for LDAP in advance: (You

will be prompted for this information later during the LDAP configuration.)

    a. Decide on a Distinguished Name (DN) suffix that will define the name space for your directory. A Distinguished Name and password are the credentials a user offers to the server when signing on from the Web browser.
Suggestions for this Distinguished Name suffix include your organizational unit (ou), organization's name (o) and country (c). In this example, we use **ou=itso,o=rochester,c=us**. Defining a suffix to the OS/400 LDAP server does not create a directory entry; a suffix simply identifies to the server that Distinguished Names in this namespace can be handled by the OS/400 LDAP server. If a user tries to sign on to your LDAP server with a different Distinguished Name, it will result in a referral to another server or the server will return a "no such object" error.

    b. Define an LDAP **administrator** Distinguished Name (DN) and password.

       A client authenticated to the server using the LDAP administrator Distinguished Name and password can create, delete, modify, and read all data in the directory.
In our example, we use **cn=Administrator** as the administrator's Distinguished Name and **ldappw** as the password.

6. You verify the local relational database directory LDAP will use for storage.

    a. In V5R1, an LDAP server and a relational database directory are automatically created.

    b. When using V4R5 Operations Navigator or later with V4R5 OS/400 or later, a new user library (QUSRDIRDB.LIB) is also automatically configured as the LDAP database library.

    c. For OS/400 V4R3 and V4R4, a screen will ask you to identify a library to contain the LDAP database files *and* specify the name for the **local relational database directory entry**. (typically the AS/400 or iSeries server name. Use the *WRKRDBDIRE* command to find this value).

7. You verify that a TCP/IP domain is configured correctly on your system, using the "Change TCP/IP Domain" command.

    a. From an iSeries Command prompt, type:

       CHGTCPDMN and press **F4**.

       Ensure that the host and domain name is set.

> **Note:** In some circumstances, the case of the domain or host name may matter. Therefore, you might want to write down whether they are in upper or lower case.

    b. Press **F3** to exit.

8. **Prior to V4R5**. You verify that SMTP information is configured with the "Change SMTP Attributes" command.

    a. From an iSeries Command prompt, type:

       CHGSMTPA and press **F4**.Use the **Page down** key until you find the **delimiter** field:

       Verify the user ID delimiter. The default is a question mark (?). (*Delimiter*: Specifies the single character to be used to separate parts of the SMTP user ID. All subsequent entries in the system and personal alias tables use this character.)

    b. Press the **Enter** key.

> **Note:** If you change the delimiter to one that is different from the default (?), *you must press* **Enter**. This sets the SMTP delimiter that may be needed for publishing the mail information to LDAP if the user does not have SMTP information in their system distribution directory entry.

9. You check the system value of QALWUSRDMN **Allow user domain objects in libraries** with the "Work with System Values" command.

    a. From an iSeries Command prompt, type:

    WRKSYSVAL SYSVAL(QALWUSRDMN)

    b. Press the **Enter** key.

    c. Use **Option 5** to display system values for **user domain objects in libraries**.

> **Note:** If you have previously changed the *QALWUSRDMN* system value from *ALL, make sure that the system library, **QDIRSRV2** is included as a value. Otherwise, you can't publish information from the System Distribution Directory (SDD) to the LDAP directory.

After you've verified that your system is ready, continue to step 2 of the workshop.

Select a country

← Technical Studio Home

Configuring the OS/400 LDAP Server

· Verify these Pre-Configuration Tasks

· Configure and start the OS/400 LDAP server

· Publish to the LDAP directory from the OS/400 SDD

· Verify the connection to the OS/400 LDAP server

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

Configure and Start the OS/400 LDAP Server
You are now ready to configure the OS/400 LDAP server. This topic is designed for configuring your LDAP server for the first time. If you are changing a configuration, be careful to consider existing settings while you follow these steps.

All Directory server configuration tasks are performed using Operations Navigator.

To configure OS/400 LDAP:

1. Open **Operations Navigator** from your client desktop. From the **START** button, select **Programs**, **IBM AS400 Client Access**, then **AS/400 Operations Navigator**.

2. In the left pane, click on the plus sign to the left of the iSeries server you wish to configure: ⊞ Sys400

3. Double-click on **Network**.

4. Double-click on **Servers**

5. Click **TCP/IP**.
   The TCP/IP server screen appears in the right pane:
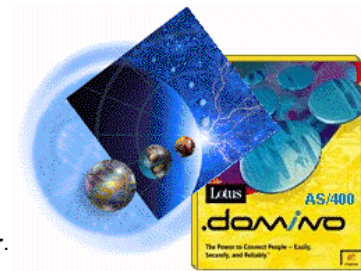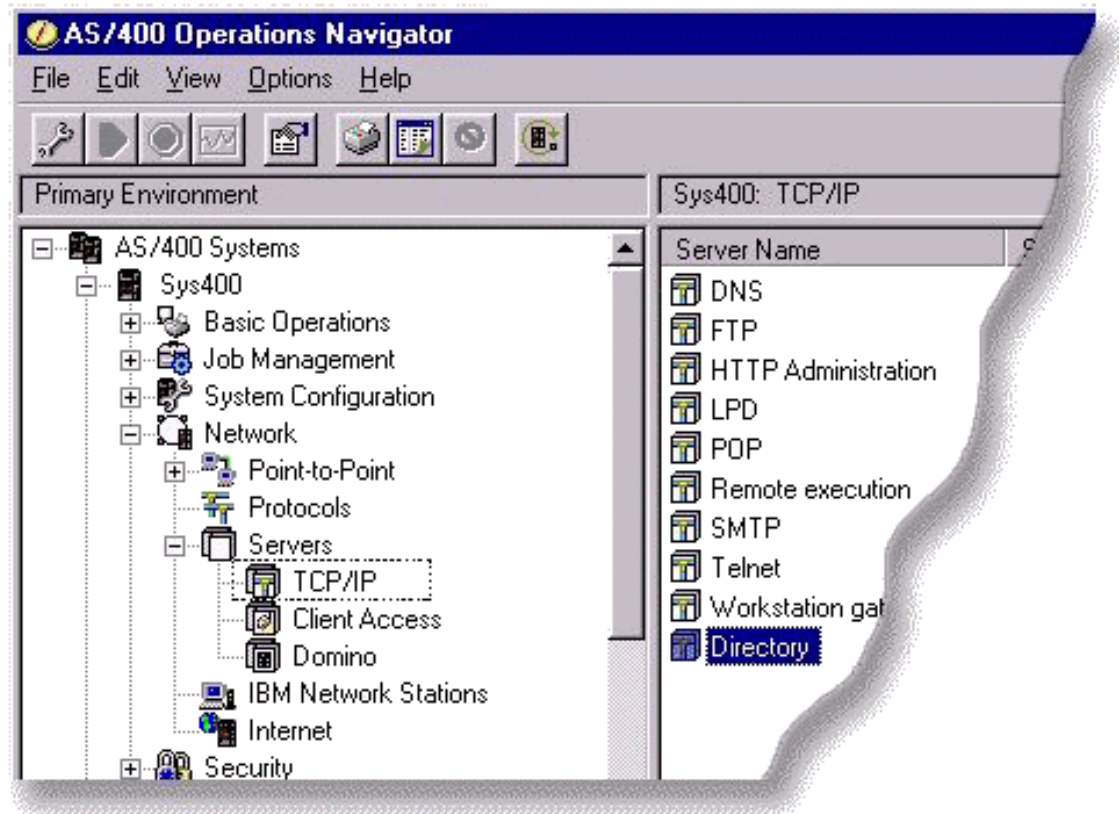
Note: If you are using **V5R1** or have already attempted configuring the Directory Server, you must stop the directory server and select the *Re-Configure* drop-down option instead. If you are simply adding a new Directory suffix, you should use the **Properties** option.
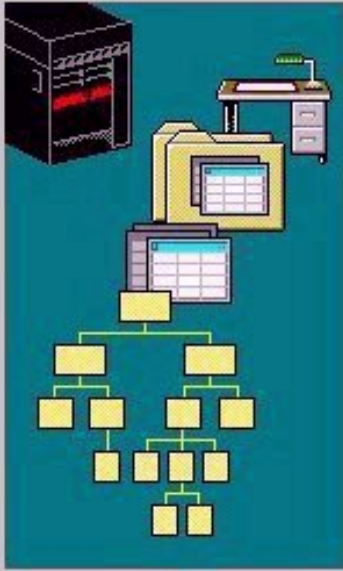
6. In the right pane, **right-click** on **Directory**, and select **Configure** from the drop-down list.

The *Configure Directory Server* wizard screen appears:
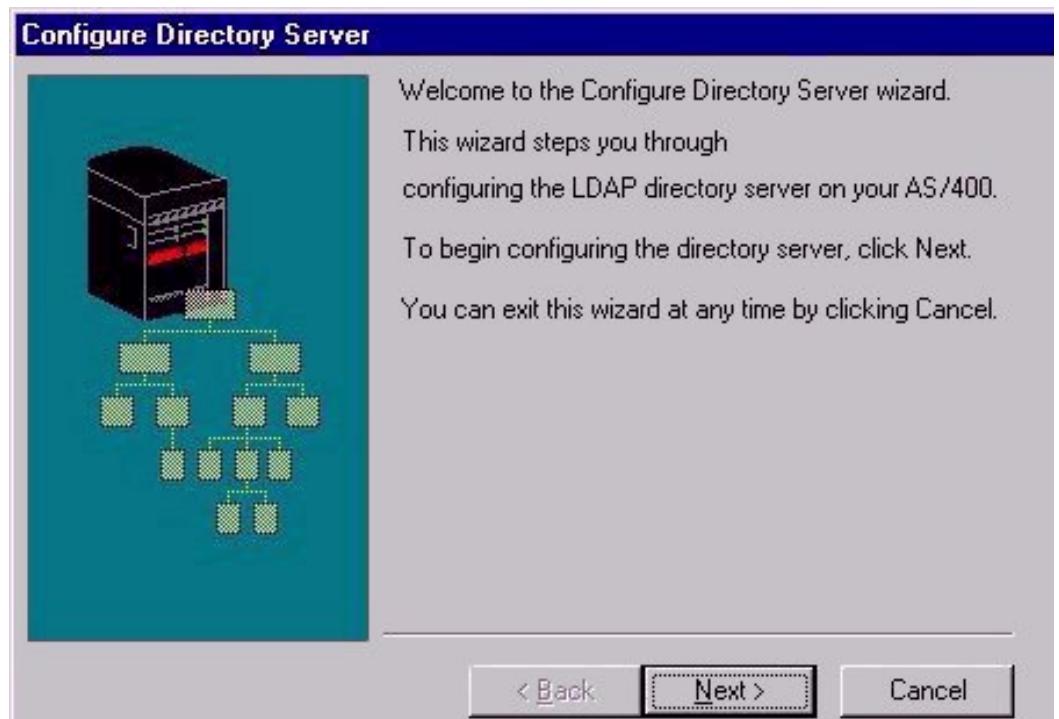
7. Click **Next>** to continue. The *Administrator Name* screen appears:
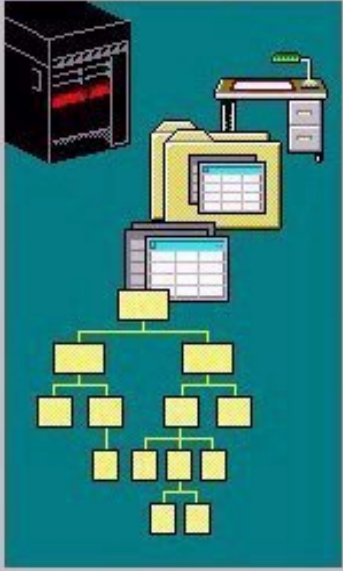
Enter the name and password for the LDAP administrator. The default name is cn=Administrator, but this can be edited. However, in our example, the default value **cn=Administrator** and a password of **ldappw** have been used.

8. Click **Next>** to continue. The *Choose Directory Suffixes* screen appears:

On the *Choose Directory Suffixes* screen, the directory suffix must be added to the directory server. Specify the lowest level of the hierarchy first. In our example, we started at the Organizational Unit (ou) of **itso**, then the Organization (o) of **rochester**, and then Country (c) of **us**.

9. Click **Add** and then click **Next>** to continue. The *Start Server when TCP/IP is Started* screen appears:
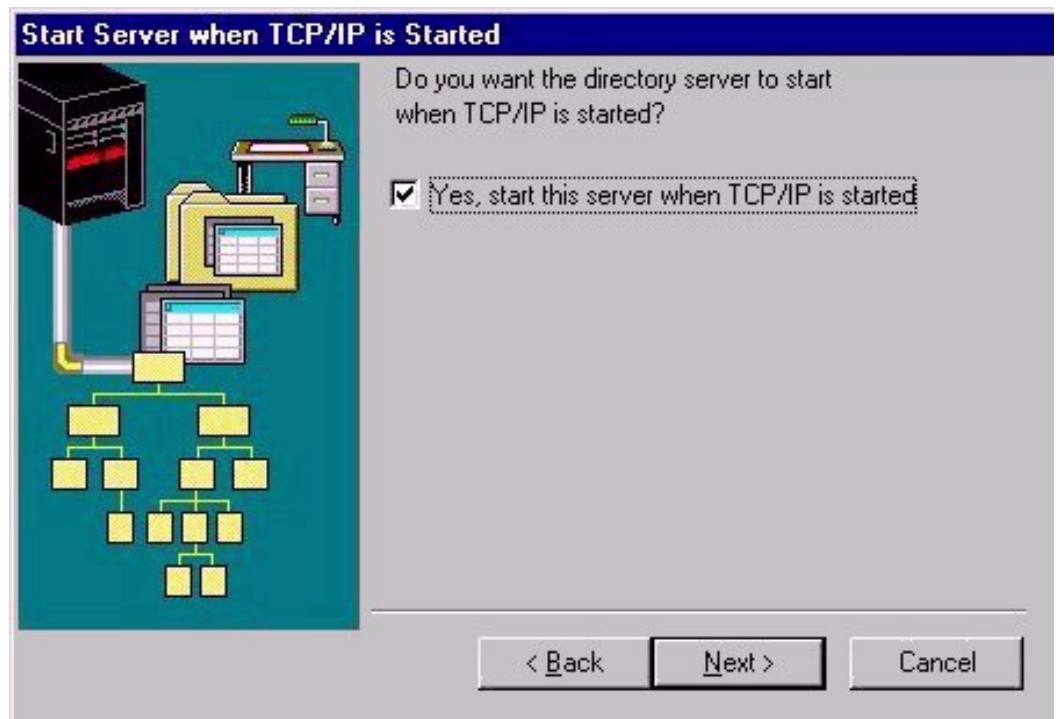
On this screen, the **Yes, start this server when TCP/IP is started** option is already checked.

Do **not** deselect this box. If you do, LDAP does not start when you start TCP/IP on your system.

10. Click **Next>** to finished configuring OS/400 LDAP. The *Configuration Summary* screen appears:
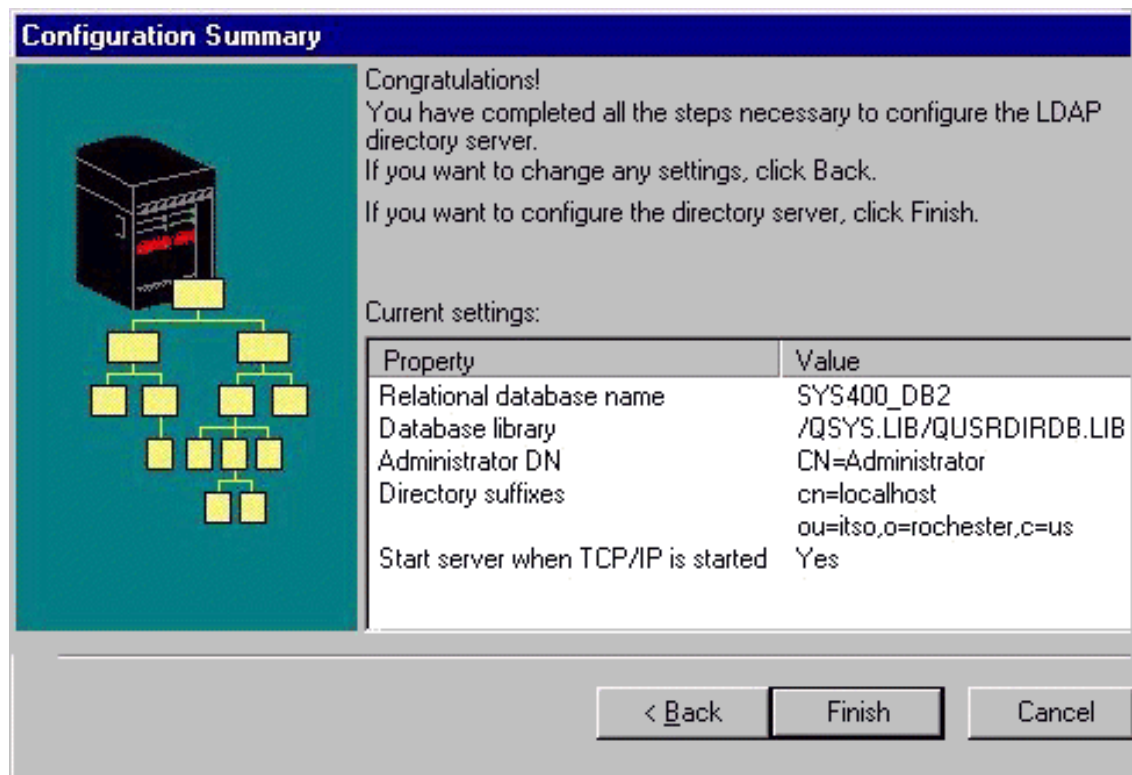
Ensure that the information is correct.

11. Click **Finish**. The Directory server is now configured.

12. To start the LDAP server from Operations Navigator.

In the right pane of Operations Navigator, **right-click** on the **Directory** server.

Select **Start**.

(If you are interested, you could
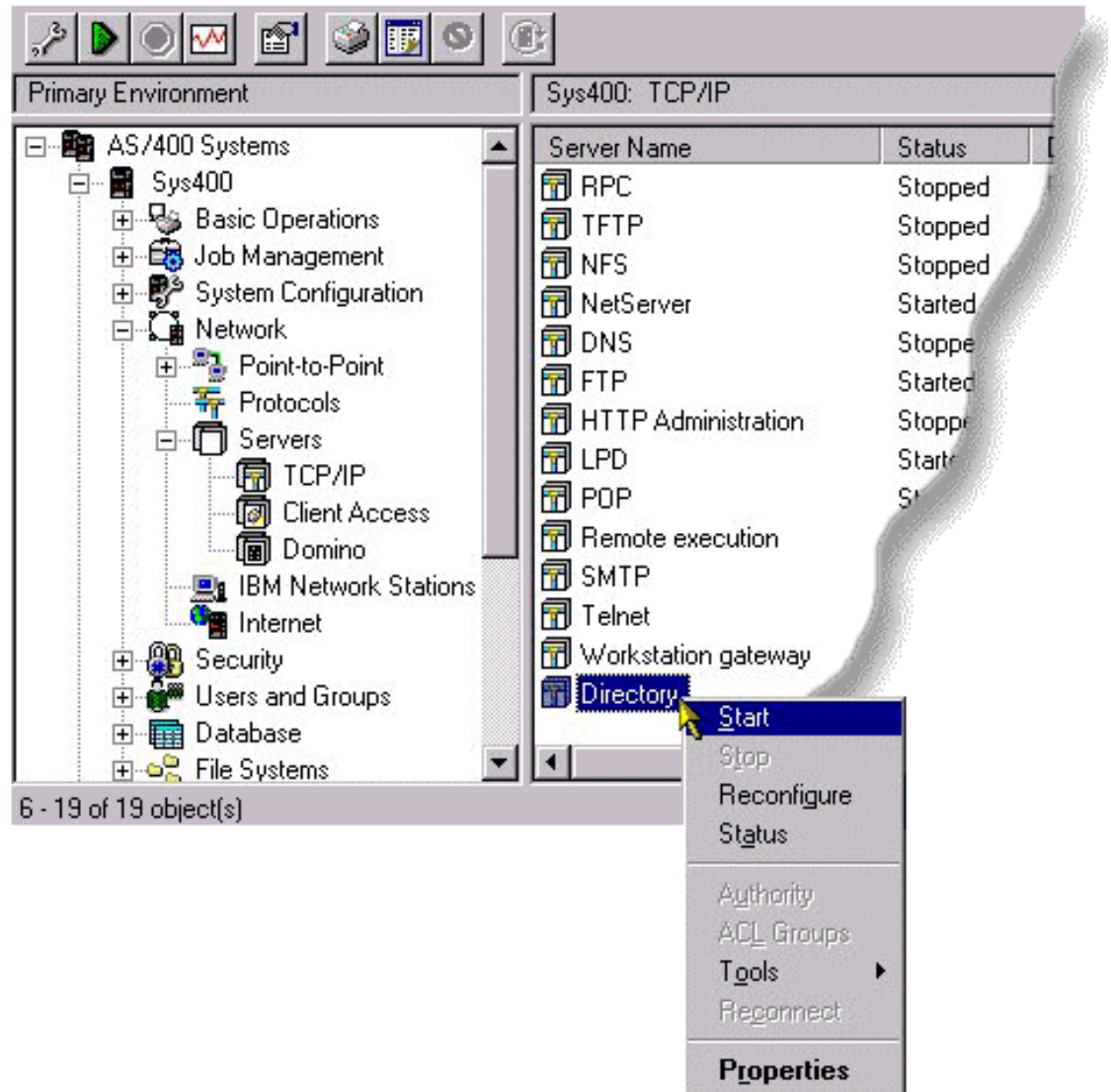
13. Be sure the Directory status changes to **Started**. You may need to use the **F5** key to refresh your screen.

This finishes configuring the OS/400 LDAP Directory Server.

In the next step you'll publish, or copy, your SDD users to the LDAP directory.

Select a country

← Technical Studio Home

Configuring the OS/400 LDAP Server

· Verify these Pre-Configuration Tasks

· Configure and start the OS/400 LDAP server

· Publish to the LDAP directory from the OS/400 SDD

· Verify the connection to the OS/400 LDAP server

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

Publish to the LDAP directory from the OS/400 SDD
You've configured and started the LDAP Directory server on your iSeries or AS/400. Now you're ready to publish your users in the OS/400 System Distribution Directory (SDD) to the new LDAP directory.

Once transferred, the SDD is automatically synchronized with the LDAP directory.

To publish your System Distribution Directory:

1. Open Operations Navigator.

    a. From the **START** button, select **Programs**, then **IBM AS400 Client Access**, then **AS/400 Operations Navigator**.
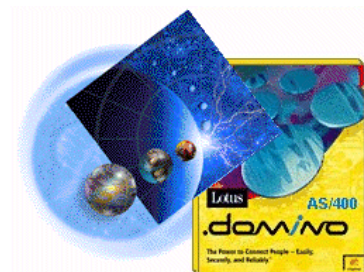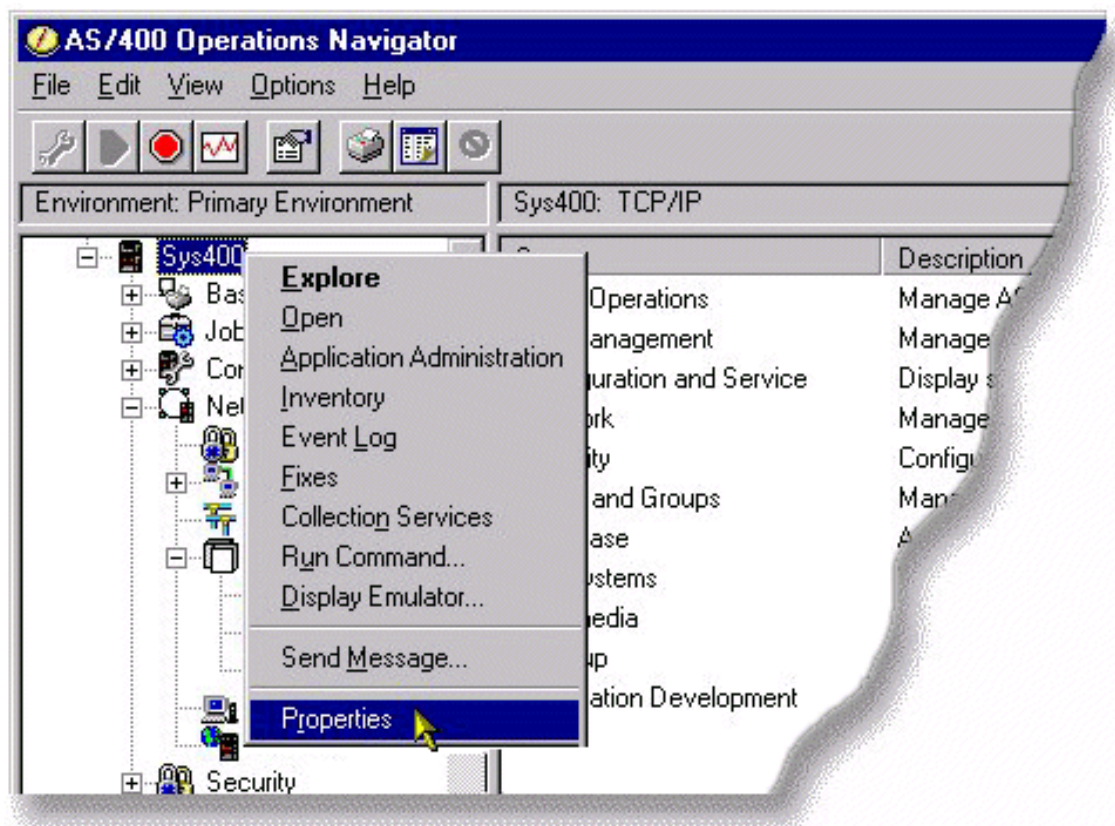
2. In the left pane, **right-click** on the system that has the SDD you want to publish.

3. Select **Properties**. The *Properties* window appears.

4. Click the **Directory Services** tab.
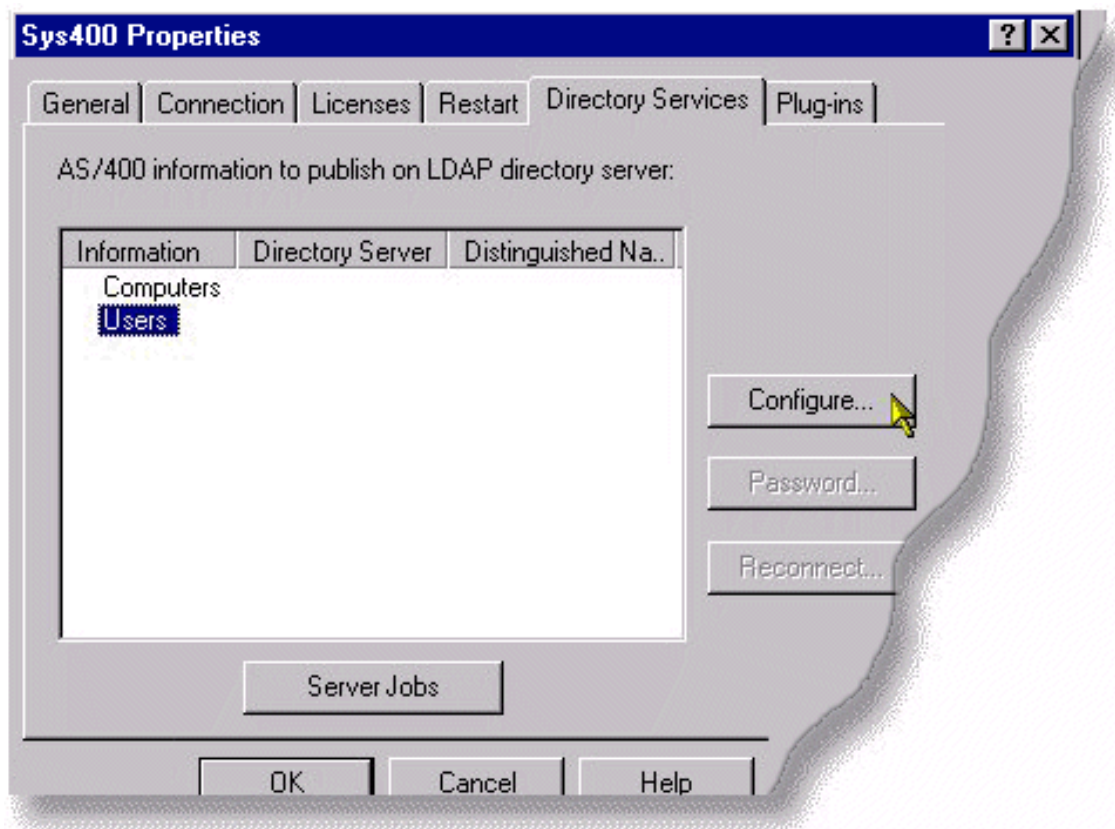
5. From the list that appears, select **Users**.

6. Click **Configure**.

The *Directory Services Publishing - Configure* window appears:

Directory Services Publishing - Configure

☑ Publish AS/400 information for:

Users

Where to publish:

Directory server: Sys400

Under DN: ou=itso,o=rochester,c=us ▼

Server connection:

Distinguished name: cn=Administrator

Password: ××××××

☐ Use Secure Sockets Layer (SSL)

Port: 389

Verify

OK   Cancel   Help

7. Select the **Publish AS/400 information for** check box.

   Enter the following values:

   ○ In the **Where to Publish** section, for the "Directory server" parameter, specify the system name that the LDAP server is running on. In our example, use **SYS400**.

   ○ For the **Under DN** parameter, enter the DN name you specified when you configured the LDAP server (e.g. **ou=itso,o=rochester,c=us**).

   ○ In the **Server Connection** section, specify the "Distinguished Name" parameter of the LDAP server administrator (e.g. **cn=Administrator**). This was created when you configured the LDAP server.

   ○ Enter the **Administrator Password** that you specified when you configured of the LDAP server (e.g. **ldappw**).

   ○ Leave the port setting at 389, since this is the default for the LDAP server.

8. Click **Verify** to make sure that the directory path you specified exists on the LDAP server.

9. If the directory path does not exist, you are prompted to create the path, as shown in this example:

Directory Services   ? X

⚠ Directory path ou=itso,o=rochester,c=us does not exist. Would you like to create it?

Yes   No

   Click **Yes**. If you do not create the path, publishing will not successful.

10. Wait for the *Directory Services settings verified successfully* message box to appear.
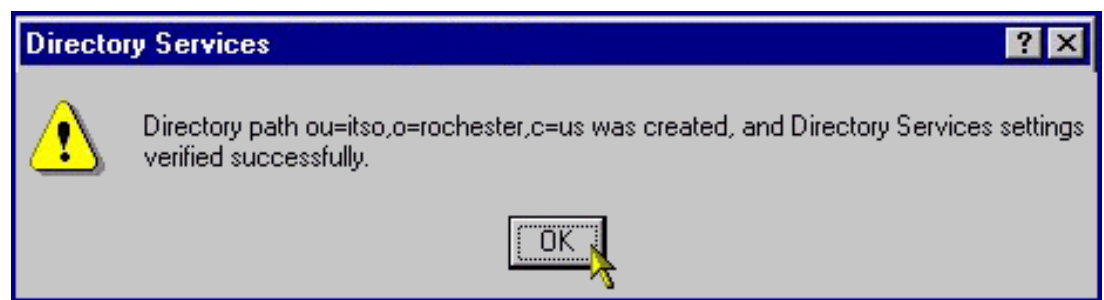
Click **OK**.

11. The *Directory Services* screen appears:
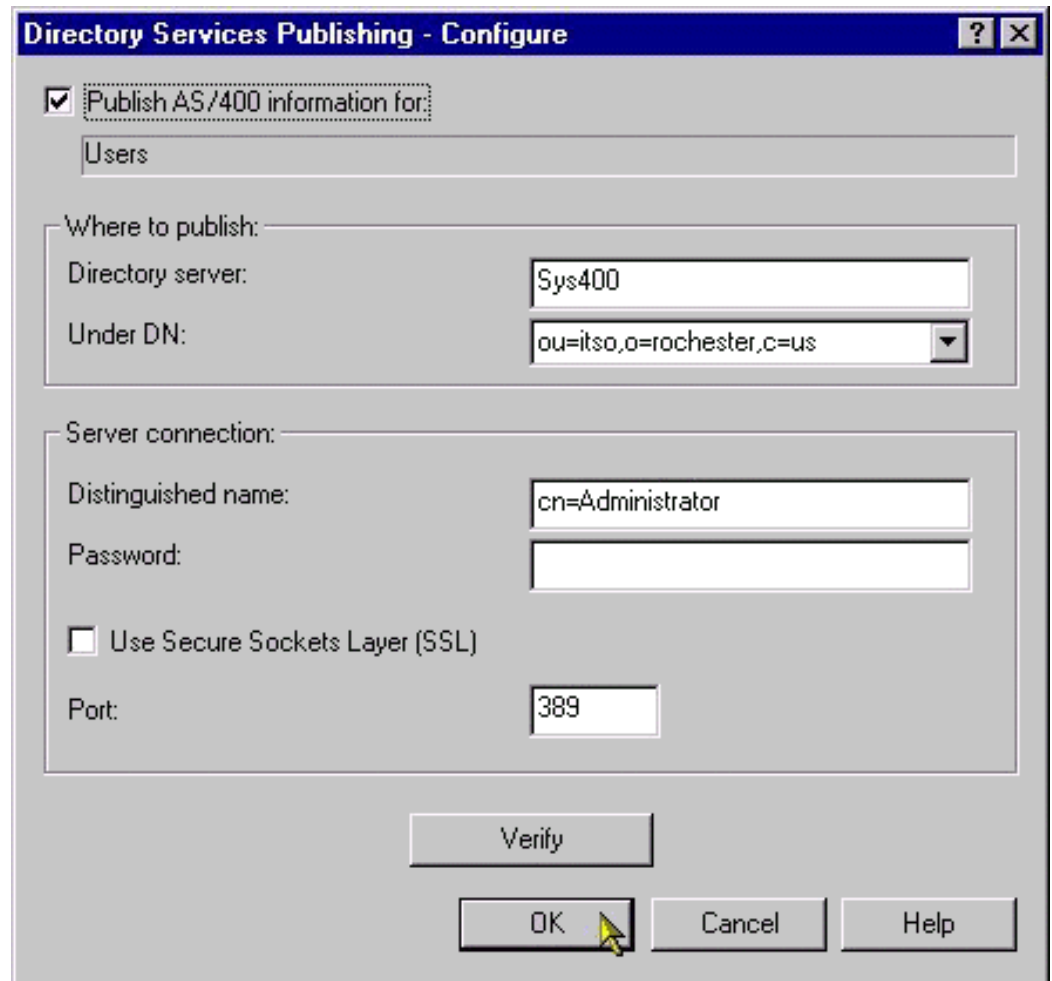
Click **OK** to exit. The SDD is synchronized with the LDAP directory every five minutes.

12. The *system properties* screen re-appears:
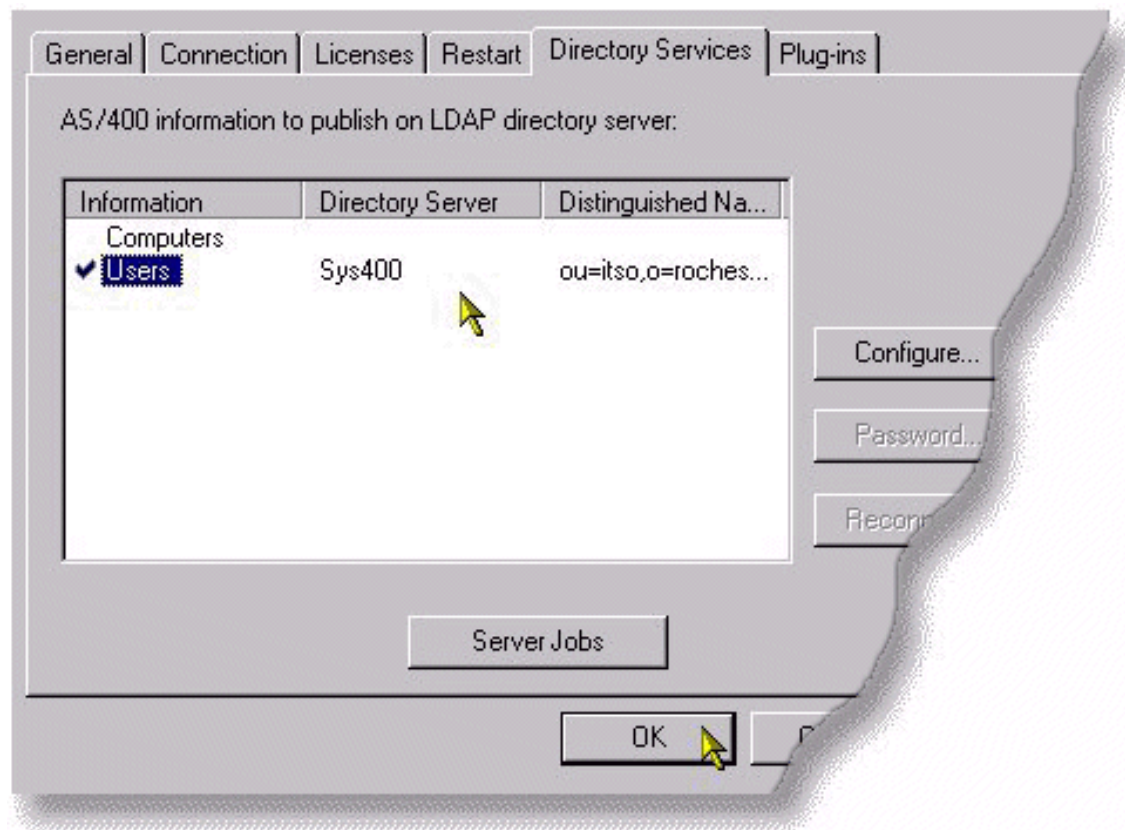
13. Click **OK**.

You have successfully published the SDD users to the LDAP directory.

Next, verify the connection to OS/400 LDAP directory.

Select a country

← Technical Studio Home

Configuring the OS/400 LDAP Server

· Verify these Pre-Configuration Tasks

· Configure and start the OS/400 LDAP server

· Publish to the LDAP directory from the OS/400 SDD

· Verify the connection to the OS/400 LDAP server

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

Verify the connection to the OS/400 LDAP server
You've configured and started the LDAP Directory server on your iSeries or AS/400. You've published the OS/400 System Distribution Directory (SDD) users to the new LDAP directory. Now you're ready to check the connection to the OS/400 LDAP directory and verify that the directory entries were published from the OS/400 System Distribution Directory (SDD).

There are a number of different methods for doing this. In these steps, you'll use your Web browser. In our example, we'll use Netscape Navigator. You could also use the Qshell utility.
You cannot verify a connection with Internet Explorer or certain newer versions of Netscape.
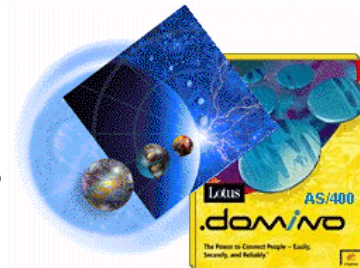
To verify a connection to LDAP from your browser:

1. Open Netscape Navigator.

2. In the **Location**, or address line of Netscape, type the location of your LDAP server:

   ldap://SYS400.IBM.COM/
   (where *SYS400.IBM.COM* is the full domain name of your iSeries or AS/400)

3. Press **Enter**.

4. Since this is the first connection to your LDAP server, a message box will appear:
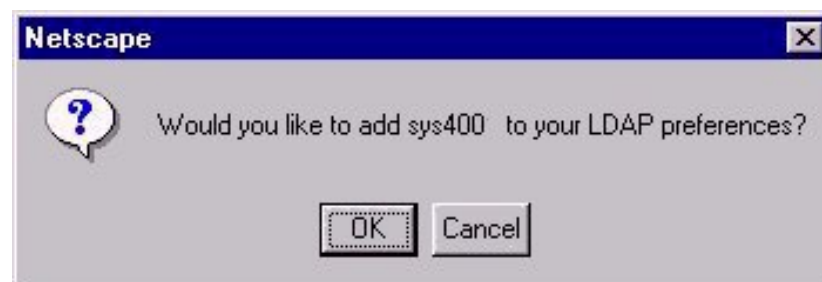
5. Click **OK**.

   You should get a screen full of information:

```
Bookmarks    Go to: ldap://SYS400.IBM.COM/

namingcontexts            CN=SCHEMA
                          OU=ITSO,O=IBM,C=US
                          CN=LOCALHOST
subschemasubentry         cn=schema
supportedcontrol          2.16.840.1.113730.3.4.2
security                  none
port                      389
supportedsaslmechanisms   CRAM-MD5
supportedldapversion      2
                          3
ibmdirectoryversion       3.1.1
```
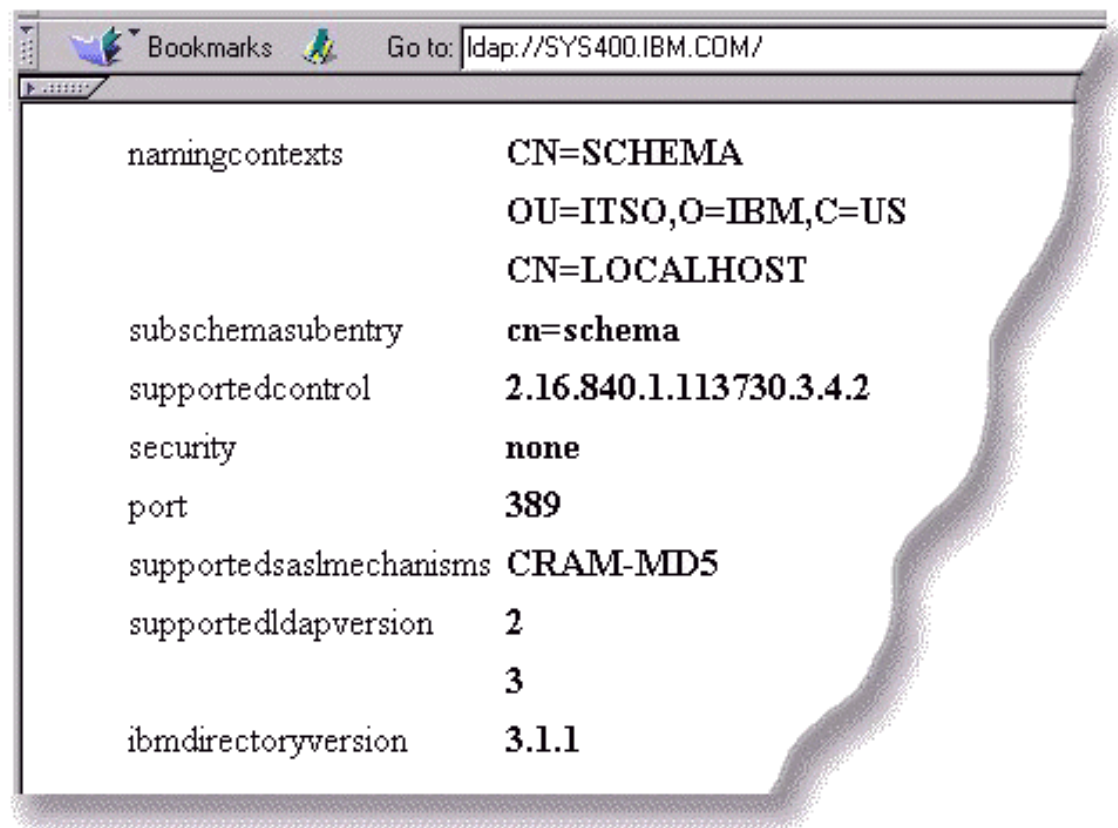
If you do not, your LDAP server is not **V5R1**, is not configured correctly, or is not started.

> **Note:** This does not work with MS Internet Explorer, and may not work with new versions of Netscape.
> You can also check the server logs with Operations Navigator V5R1.

6. To verify that your OS/400 user ID has been published from the System Distribution Directory (SDD) to the new LDAP directory.

   Enter this information in the Netscape location:

   ldap://*SYS400*/cn=*Joe Admin*,ou=*itso*,o=*rochester*,c=*us*
   (where *SYS400, Joe Admin, itso, rochester, & us* are entries from your own system).

7. Press **Enter**. You will see a screen that displays the User ID information.
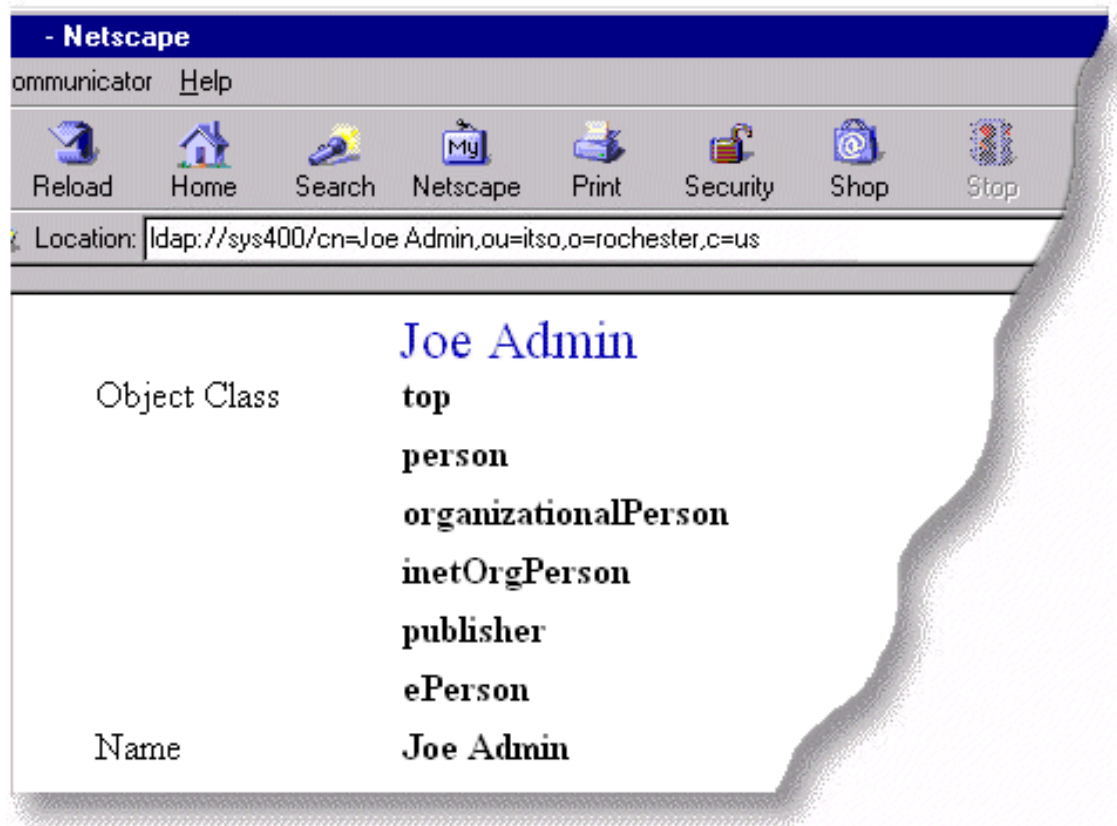
If you do not get the users information, you may need to add the user to the System Distribution Directory (SDD). A Technical Studio topic on adding users to the SDD can be found in *e-business 101* lesson 3.

Check out this LDAP "Question and Answers" page for a setup checklist:
http://www.ibm.com/servers/eserver/iseries/ldap/ldapfaq.htm

Now, you have verified the LDAP directory.

Congratulations! You have finished configuring your iSeries or AS/400 LDAP directory services.

Select a country

← Technical Studio Home

Configuring the OS/400 LDAP Server

· Verify these Pre-Configuration Tasks

· Configure and start the OS/400 LDAP server

· Publish to the LDAP directory from the OS/400 SDD

· Verify the connection to the OS/400 LDAP server

Download PDF version 1.2Mb

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

LDAP (Lightweight Directory Access Protocol)
According to the iSeries 400 Directory Services Home page:

"Directory Services provides Lightweight Directory Access Protocol (LDAP) on the OS/400 which includes both AS/400 and iSeries 400. Directory Services is part of the IBM SecureWay® Directory family of products and services and is sometimes referred to as SecureWay Directory for OS/400. LDAP runs over Transmission Control Protocol/Internet Protocol (TCP/IP), and is gaining popularity as a directory service for both Internet and non-Internet applications. You perform most setup and administering tasks of the LDAP directory server through the graphical user interface (GUI) of Operations Navigator for OS/400. To administer Directory Services, you must have Operations Navigator installed on a PC that is connected to your system. You can use Directory Services with LDAP-enabled applications, such as mail applications that look up e-mail addresses from LDAP servers. Since V4R3, LDAP has been included free in OS/400 as part of Directory Services for OS/400 (BOSS option 32). Directory Services includes an LDAP server and complete set of LDAP clients and utilities. "
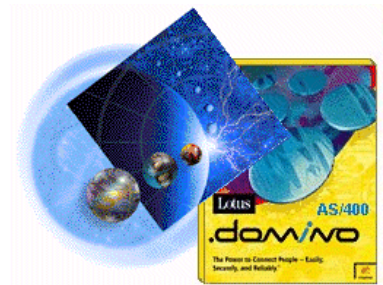
Another quote from the *Lotus Notes Administrative Client Help Glossary*:
"LDAP is a set of protocols for accessing information directories. LDAP is based on the X.500 protocol, but supports TCP/IP, which is necessary for Internet access. Because it's a simpler version of X.500, LDAP is sometimes called X.500-lite. You can enable LDAP on a Domino server to allow LDAP clients to access information in the Domino Directory, for example, e-mail addresses."

LDAP directory
A hierarchical directory of names that can reflect an organization's structure or geography and that is accessed via the LDAP protocol.

Running LDAP on a Domino server enables the Domino Directory, or address book, to serve as an LDAP directory and be accessible from the iSeries through intranet or Internet sites.

Two popular public LDAP directories are Bigfoot and Four11.

Another LDAP definition page can be found at the Univ. of Michigan

About IBM | Privacy | Legal | Contact

Configuring the OS/400 LDAP Server

· Verify these Pre-Configuration Tasks

· Configure and start the OS/400 LDAP server

· Publish to the LDAP directory from the OS/400 SDD

· Verify the connection to the OS/400 LDAP server

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

Start and Monitor OS/400 LDAP Using a 5250 (green screen) Session
Using a 5250 (green screen) session to start and view the status of the OS/400 LDAP server.

To start the LDAP directory server using a "Start TCP/IP Server" command:

1. Open a 5250 (green screen) session. In our example, we'll use Client Access.

```
                                    Command Entry

Previous commands and messages:

    (No previous commands or messages)











Type command, press Enter.
===> STRTCPSVR *DIRSRV



F3=Exit    F4=Prompt    F9=Retrieve    F10=I
F11=Display full         F12=Cancel     F13=
```

2. From an OS/400 command line, type:

   STRTCPSVR *DIRSRV

3. Press the **Enter** key.
   The LDAP directory server will start.

```
                        Command Entry

Previous commands and messages:
    > STRTCPSVR *DIRSRV
      DIRSRV server starting.




Type command, press Enter.
===> WRKACTJOB SBS(QSYSWRK)
_____
_____
_____
_____
F3=Exit    F4=Prompt    F9=Retrieve    F10=Ir
F11=Display full          F12=Cancel    F13=
```

To view and monitor the status of the LDAP directory server in the QDIRSRV job, use the "Work with Active Job" command.

    4. From an OS/400 command line, type:

       WRKACTJOB SBS(QSYSWRK)

    5. Press the **Enter** key.

       The *Work with Active Job* screen appears listing the jobs associated with QDIRSRV:

```
                              Work with Active Jobs

CPU %:      .0      Elapsed time:    00:00:00        Active j

Type options, press Enter.
  2=Change    3=Hold    4=End    5=Work with    6=Release
  8=Work with spooled files    13=Disconnect ...

Opt   Subsystem/Job   User        Type   CPU %   Functio
__    QSYSWRK         QSYS        SBS      .0
__      QDIRSRV       QDIRSRV     BCH      .0     PGM-QG
__      QGLDPUBA      QDIRSRV     ASJ      .0     PGM-QG
__      QGLDPUBE      QDIRSRV     ASJ      .0     PGM-QG
__      QIJSSCD       QIJS        BCH      .0     PGM-Q
__      QMSF          QMSF        BCH      .0
__      QNEOSOEM      QUSER       ASJ      .0     PG
__      QNEOSOEM      QUSER       BCH      .0     F
__      QNEOSOEM      QUSER       BCH      .0     F

Parameters or command
===> _____
F3=Exit    F5=Refresh          F7=Find        F1
F11=Display elapsed data    F12=Cancel        F
```

6. Press **F3** to exit.

Use your browsers **BACK** button to return to the LDAP configuration page.

Select a country
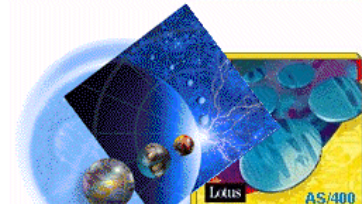
← Technical Studio Home

Configuring the OS/400 LDAP Server

· Verify these Pre-Configuration Tasks

· Configure and start the OS/400 LDAP server

· Publish to the LDAP directory from the OS/400 SDD

· Verify the connection to the OS/400 LDAP server

Download PDF version 1.2Mb

Related links:

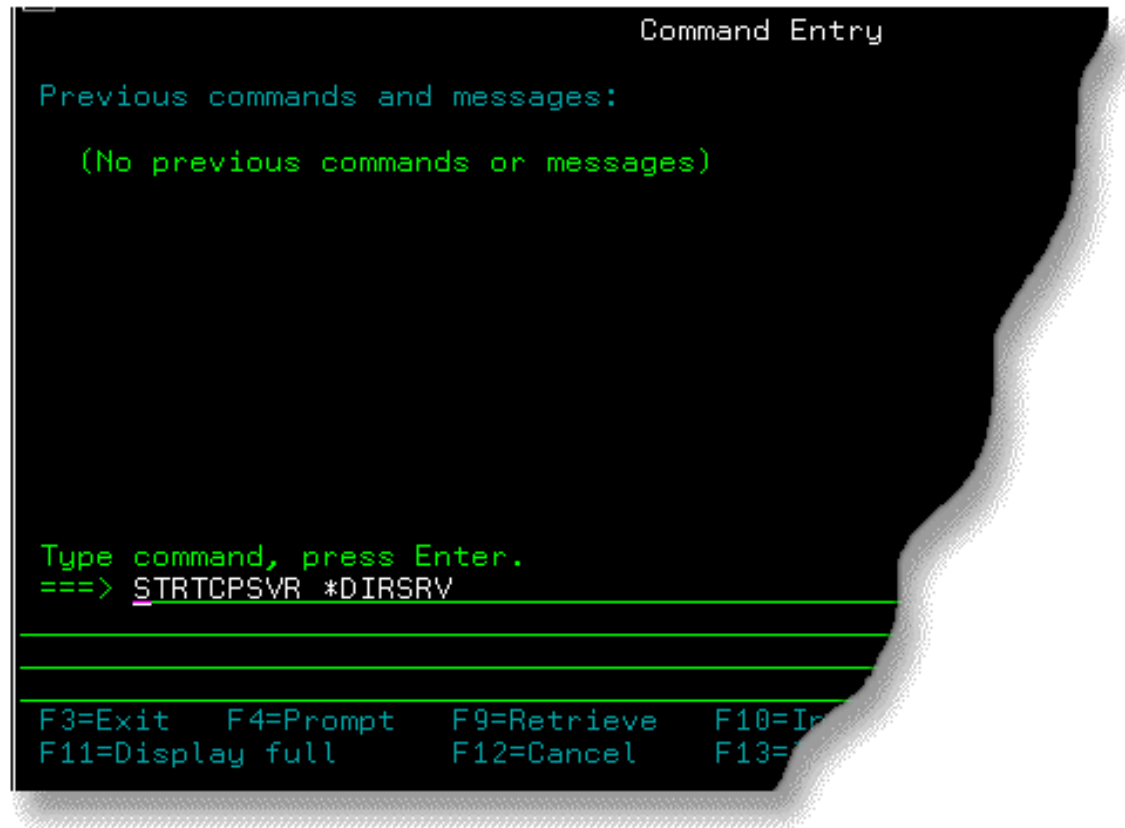iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

Description of the System Distribution Directory (SDD)
According to Redbook GG24-4449-00 Appendix C:

"The system distribution directory is supplied with OS/400. There may be other directories that exist on the AS/400, but there is only one system distribution directory. We only discuss the system distribution directory here and refer to it as the directory. The directory contains a collection of entries for users on both the local system and remote systems that are authorized to send and receive distributions on the network. Distributions are defined to be messages, data or objects that are sent between network users.

Each entry in the system distribution directory contains information about a network user. This information includes the user¢s ID and address along with a textual description. Optional fields for each entry specify information such as the network user¢s E-mail addresses (for example, X.400 O/R address or SMTP address).

You can add, change, and remove entries from the local system distribution directory. Also, entries from system distribution directories located on remote AS/400s can be shadowed to the local system. Directory shadowing provides a method to share directory information among AS/400s in a network. If a directory entry is added, removed, or modified on any AS/400 in the network, the change can be sent (shadowed) to the other AS/400s in the network."

Additional References:

● SNADS - Configuring and Setting Up SNA Distribution Services

● iSeries 400 Directory Services (LDAP)
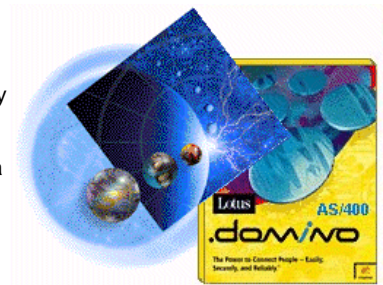
← Technical Studio Home

Configuring the OS/400 LDAP Server

- Verify these Pre-Configuration Tasks

- Configure and start the OS/400 LDAP server

- Publish to the LDAP directory from the OS/400 SDD

- Verify the connection to the OS/400 LDAP server

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

Verify the connection to the OS/400 LDAP server - Using Qshell
You've configured and started the LDAP Directory server on your iSeries or AS/400. You've published the OS/400 System Distribution Directory (SDD) users to the new LDAP directory. Now you're ready to check the connection to the OS/400 LDAP directory and verify that the directory entries were published from the OS/400 System Distribution Directory (SDD).

Here, we show another option: verifying the connection using the **Qshell** utility.

To check whether you can get a connection to the LDAP server and access OS/400 LDAP from the Qshell utility.

1. Open a 5250 (green screen) session. In our example, we'll use Client Access.
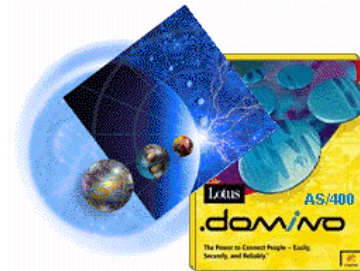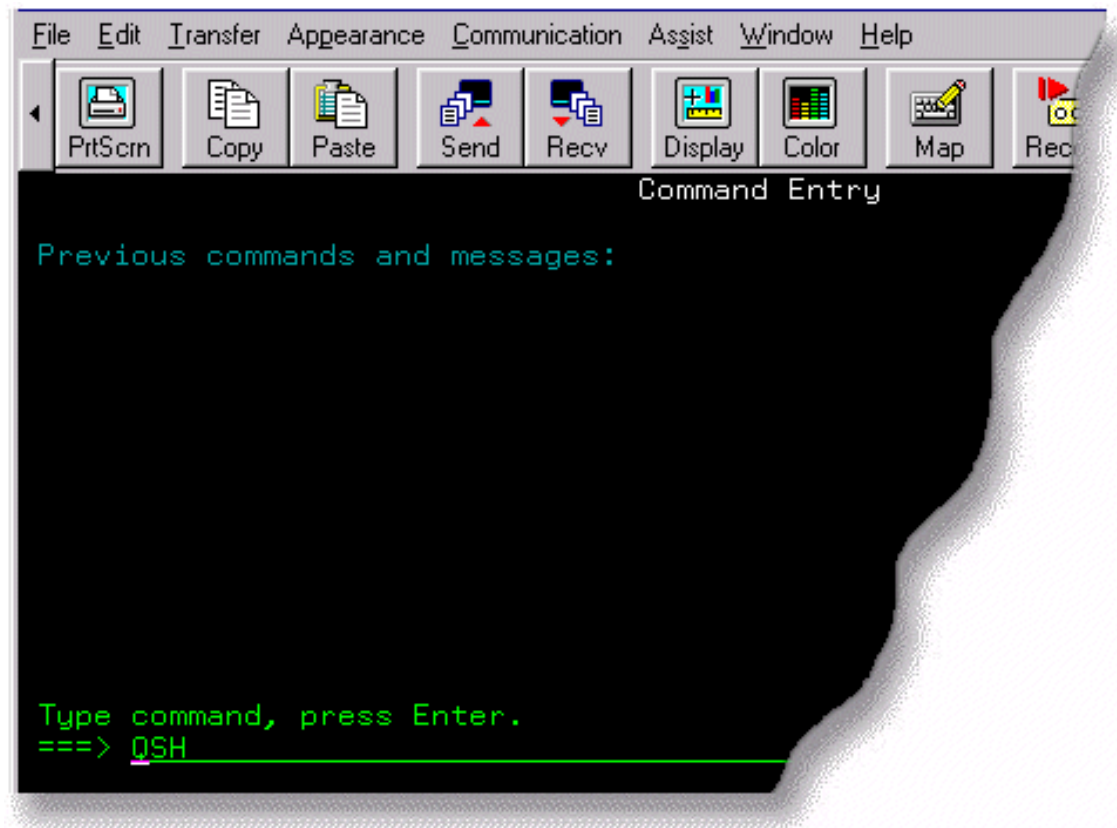
2. From an OS/400 command line, type:

   QSH
   (or STRQSH)

3. Press the **Enter** key.

   The Qshell interpreter screen will appear:
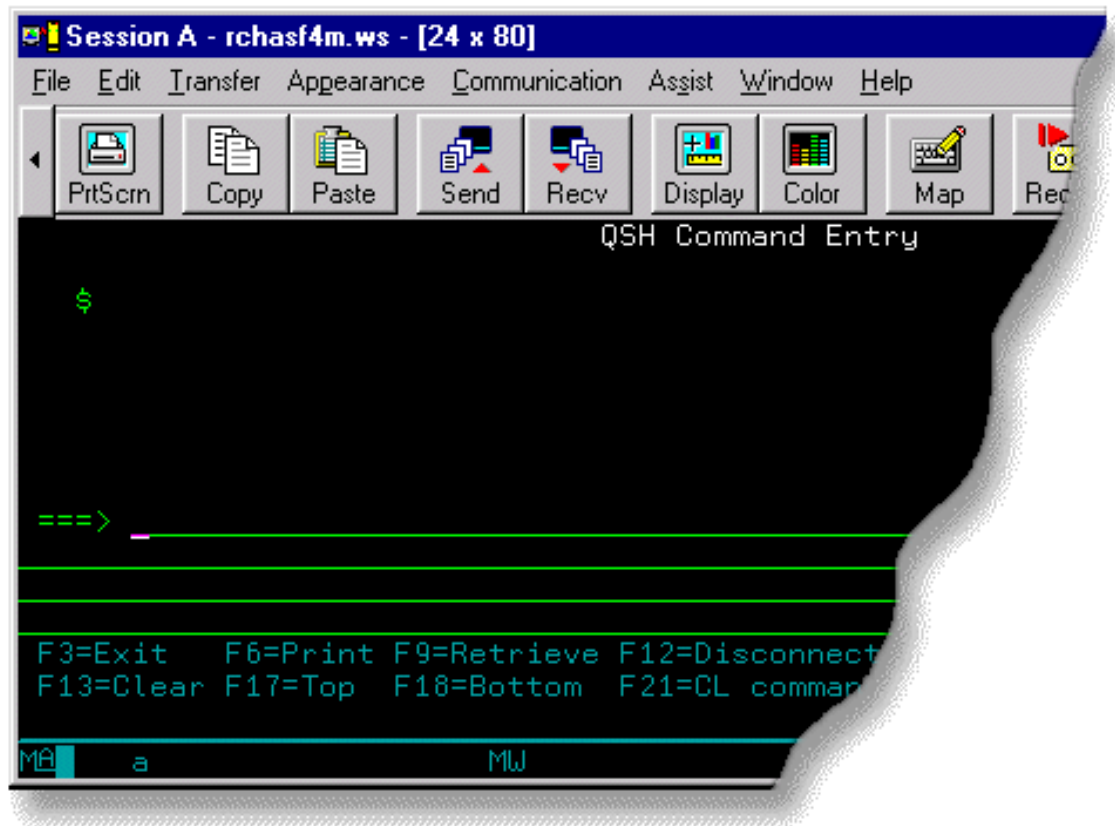
4. To check that the Administrator password is correct, enter this command information:
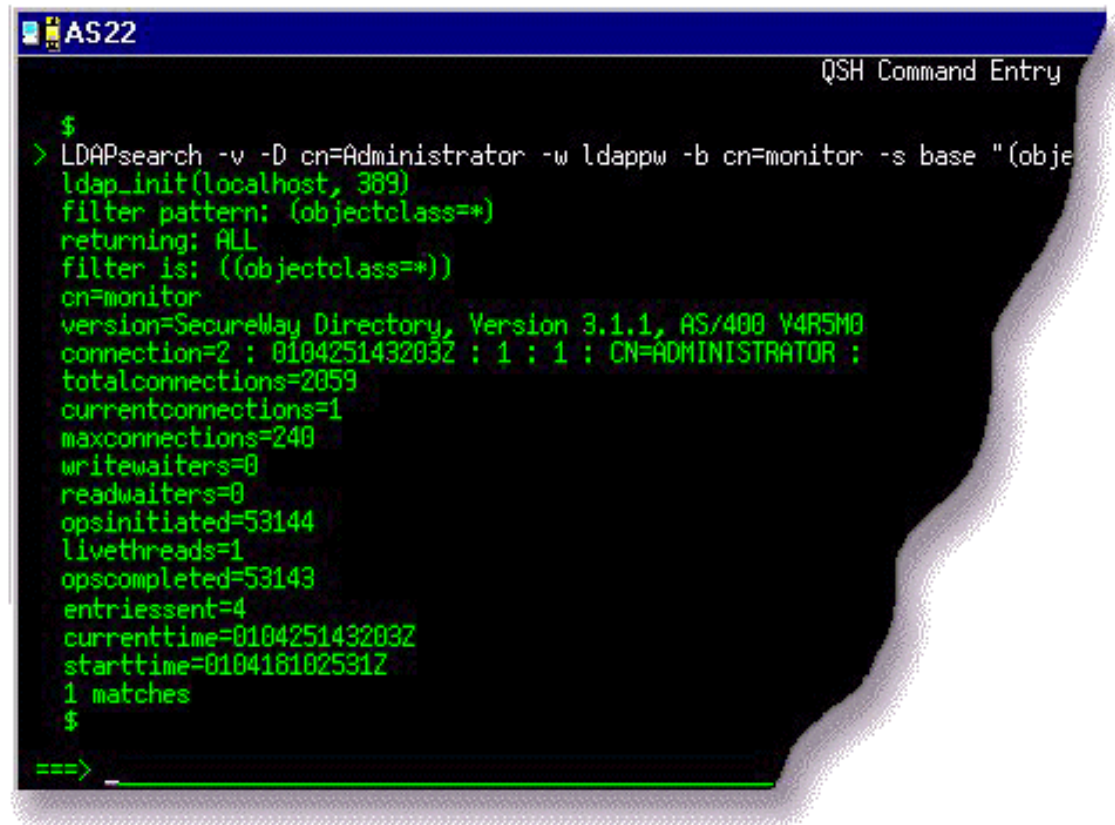
   ldapsearch -v -D cn=Administrator -w ldappw -b cn=monitor -s base "(objectclass=*)"

   The command may wrap around the command line.
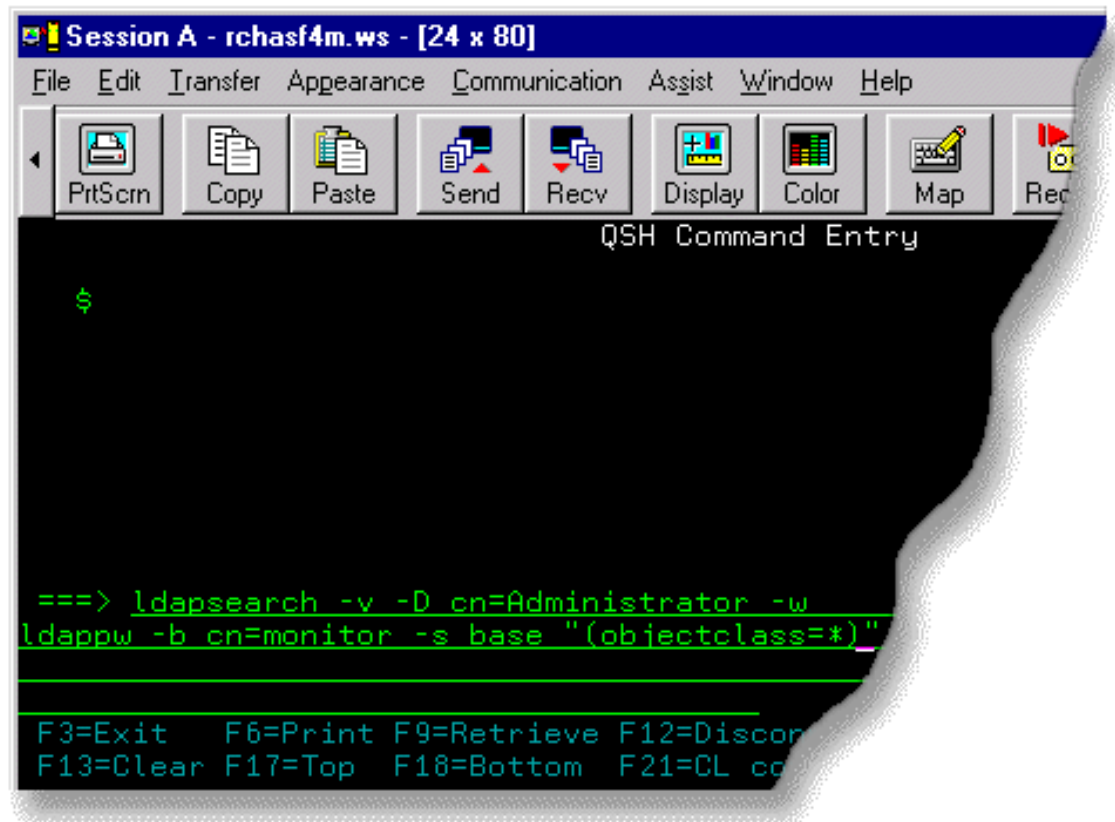
5. Press the **Enter** key.

You should get a message similar to this in reply, if the password is correct:

```
AS22                                                    QSH Command Entry

  $
> LDAPsearch -v -D cn=Administrator -w ldappw -b cn=monitor -s base "(obje
  ldap_init(localhost, 389)
  filter pattern: (objectclass=*)
  returning: ALL
  filter is: ((objectclass=*))
  cn=monitor
  version=SecureWay Directory, Version 3.1.1, AS/400 V4R5M0
  connection=2 : 010425143203Z : 1 : 1 : CN=ADMINISTRATOR :
  totalconnections=2059
  currentconnections=1
  maxconnections=240
  writewaiters=0
  readwaiters=0
  opsinitiated=53144
  livethreads=1
  opscompleted=53143
  entriessent=4
  currenttime=010425143203Z
  starttime=010418102531Z
  1 matches
  $

===> _
```

6. To search and display all directory entries, enter this command information:

   **ldapsearch -v -D cn=Administrator -w ldappw -b ou=itso,o=rochester,c=us
   "(objectclass=*)"**

   The command may wrap around the command line:

```
Session A - rchasf4m.ws - [24 x 80]

File  Edit  Transfer  Appearance  Communication  Assist  Window  Help

[PrtScrn] [Copy] [Paste] [Send] [Recv] [Display] [Color] [Map] [Rec
                                    QSH Command Entry

  $




===> dapsearch -v -D cn=Administrator -w
ldappw -b ou=itso,o=rochester,c=us
"(objectclass=*)"


F3=Exit    F6=Print F9=Retrieve F12=Discor
F13=Clear F17=Top  F18=Bottom  F21=CL co
```
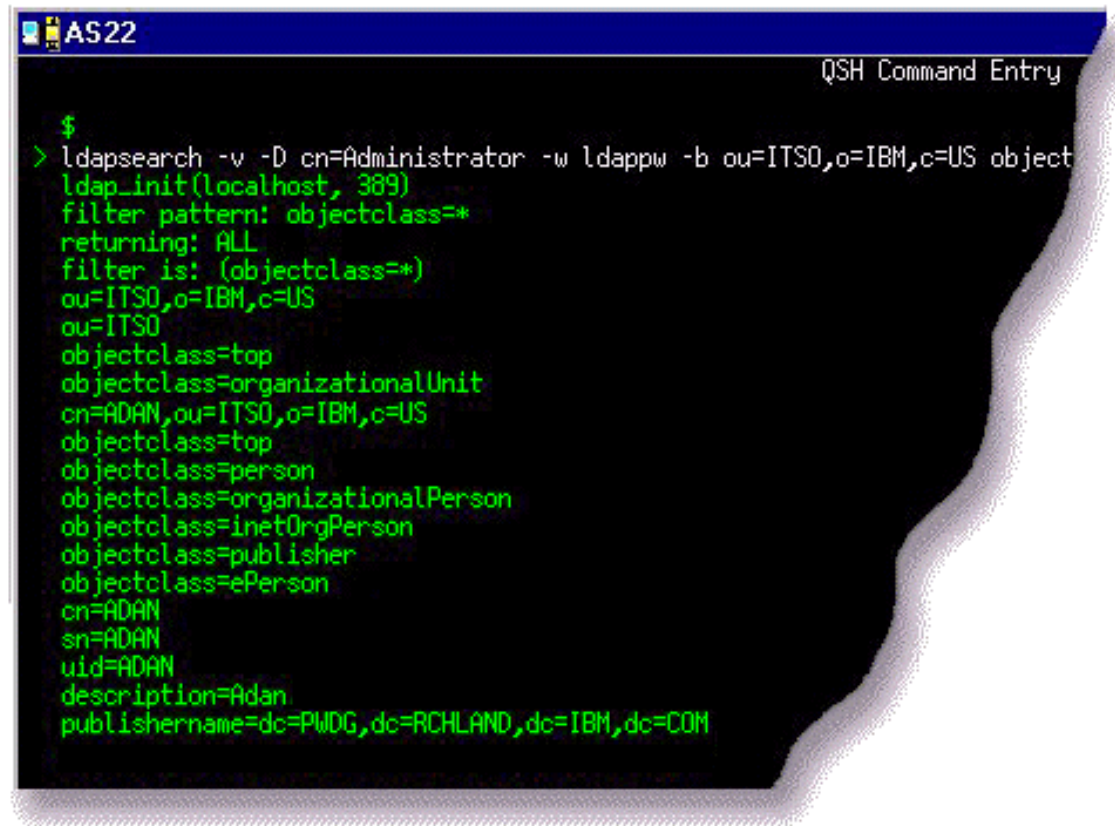
7. Press the **Enter** key.

You should get this message in reply:

```
AS22
                                                    QSH Command Entry

$
> ldapsearch -v -D cn=Administrator -w ldappw -b ou=ITSO,o=IBM,c=US object
ldap_init(localhost, 389)
filter pattern: objectclass=*
returning: ALL
filter is: (objectclass=*)
ou=ITSO,o=IBM,c=US
ou=ITSO
objectclass=top
objectclass=organizationalUnit
cn=ADAN,ou=ITSO,o=IBM,c=US
objectclass=top
objectclass=person
objectclass=organizationalPerson
objectclass=inetOrgPerson
objectclass=publisher
objectclass=ePerson
cn=ADAN
sn=ADAN
uid=ADAN
description=Adan
publishername=dc=PWDG,dc=RCHLAND,dc=IBM,dc=COM
```

If you do not get these messages, there is a problem with the LDAP configuration.
You can check the server logs with Operations Navigator V5R1 for clues to the
problem.

This completes verification of the LDAP directory using OS/400 QSHELL.

Congratulations! You have finished configuring your iSeries or AS/400 LDAP directory services.

← Technical Studio Home

Configuring the OS/400 LDAP Server

· Verify these Pre-Configuration Tasks

· Configure and start the OS/400 LDAP server

· Publish to the LDAP directory from the OS/400 SDD

· Verify the connection to the OS/400 LDAP server

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

Troubleshooting tips and server logs.
IF you are having trouble getting a response from the LDAP server, you can check the server log "print outs" for more information. If these reports are not set up to print, you can still find out their contents in Operations Navigator.
You can also use the 5250 (green screen) Qshell utility to explore more server responses.

A. Use Operations Navigator V5R1 to examine the server log "print outs" that are created by a server error:

1. Open **Operations Navigator** from your client desktop.

   a. From the **START** button, select **Programs**, then **IBM AS400 Client Access**, then **AS/400 Operations Navigator**.

2. In the left pane, click on the plus sign to the left of the iSeries server you wish to configure. ⊞ 🖳 Sys400

3. Double-click on **Network**.

4. Double-click on **Servers**

5. Click **TCP/IP**.
   The TCP/IP server screen appears in the right pane:
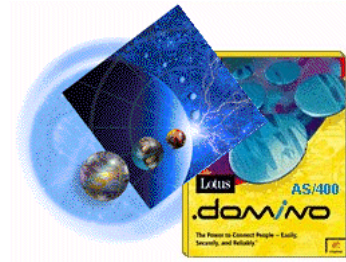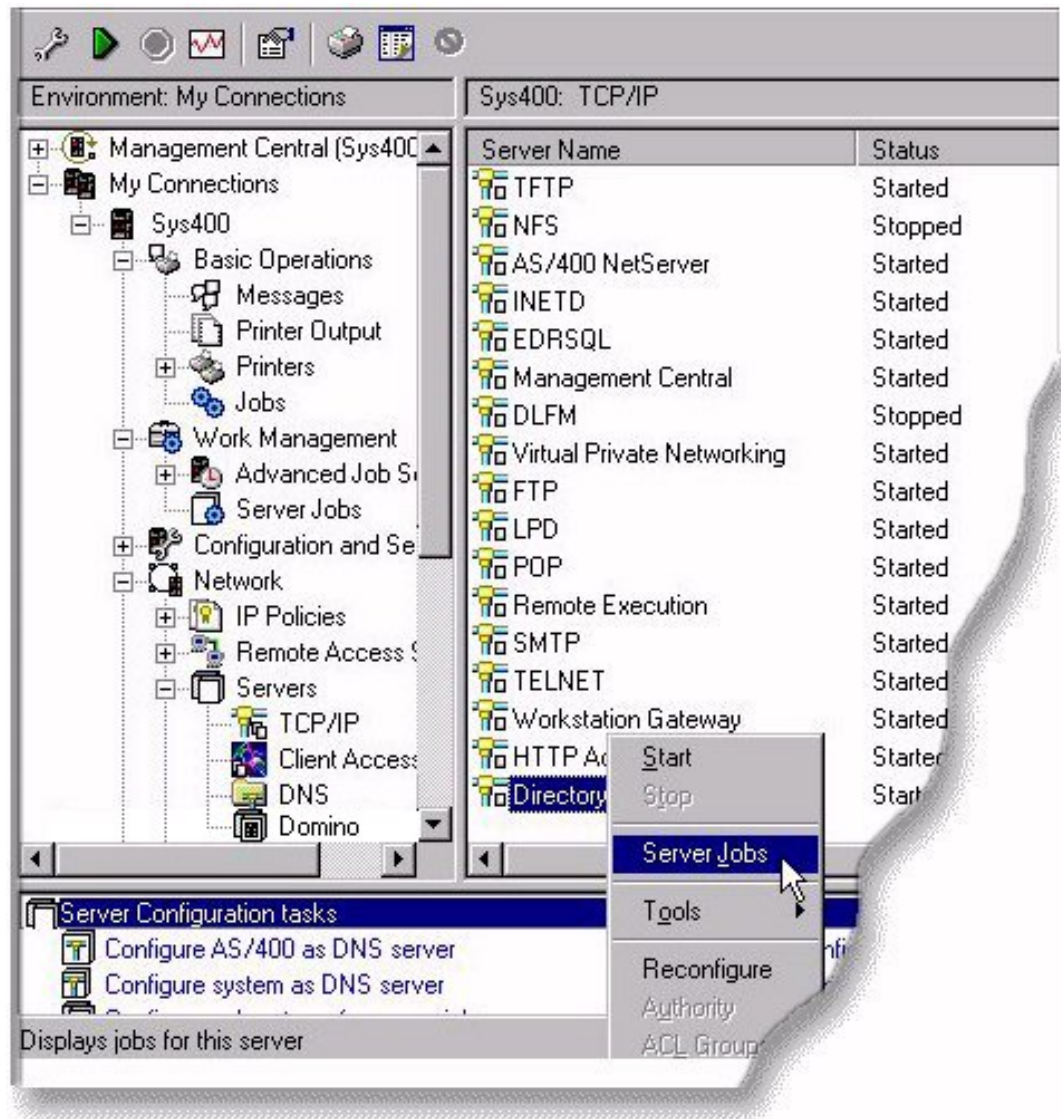
6. In the right pane, **right-click** on **Directory**, and select **Server Jobs** from the drop-down list.
   The *Active Server Jobs* screen appears:
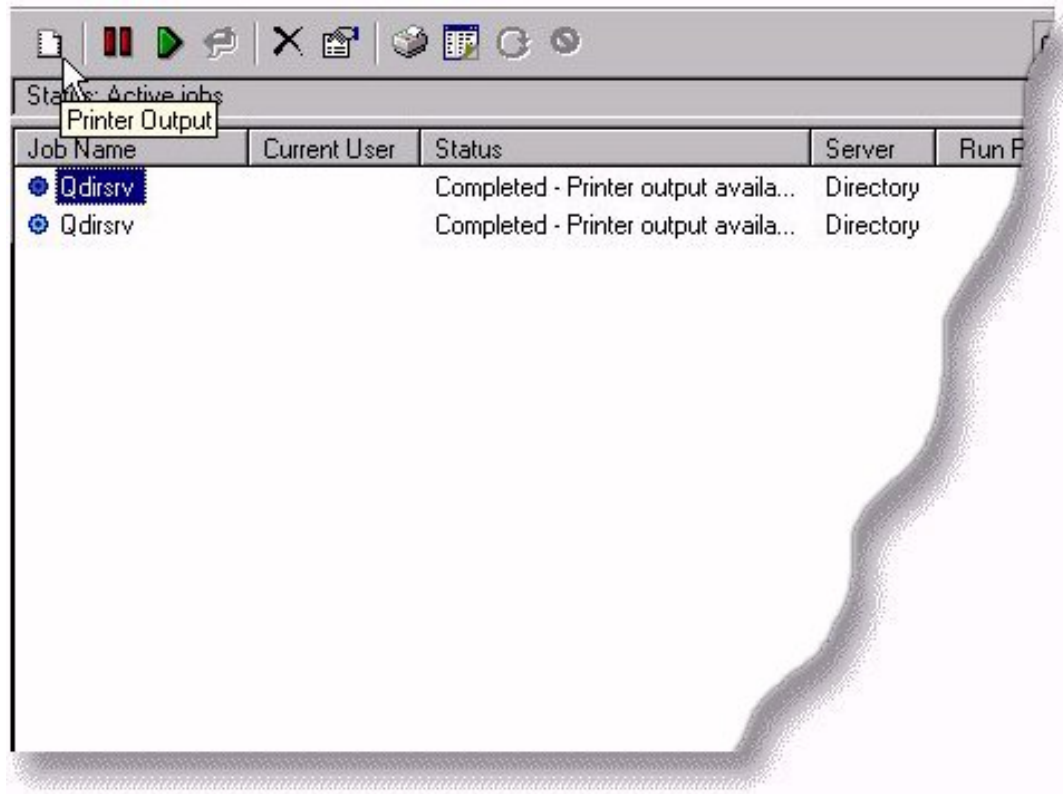
7. Select the latest **Qdirsvr** job, with a Status of **Completed - Printer output available**.

8. Click on the **Printer Output** icon in the tool bar. A screen with the job log printouts appears:
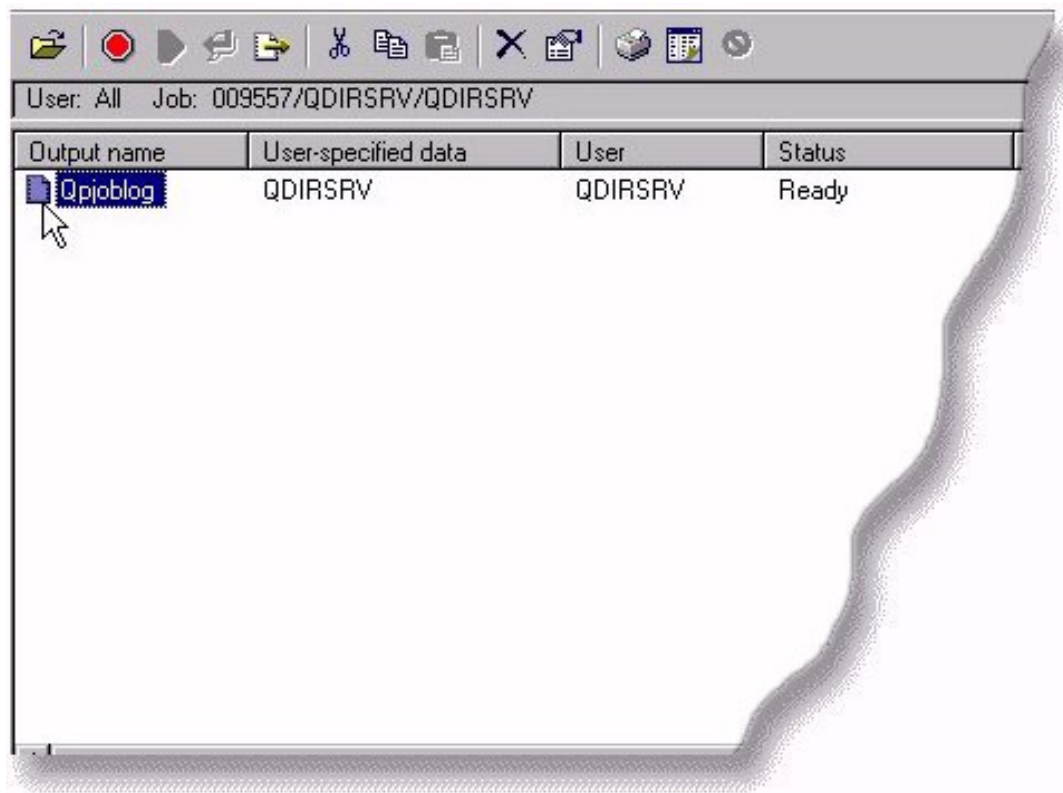
9. **Double-click** on the **Printer Output** icon. A printer output *viewer* opens:

```
Viewer - QPJOBLOG/1/QDIRSRV/009557/QDIRSRV/SYS400

File   Edit   View   Search   Notes   Options   Help

From module . . . . . . . . :      GLDSLSOC
 From procedure . . . . . . :      SocketInit
Statement . . . . . . . . . :      1279
To module . . . . . . . . . :      GLDSLSOC
To procedure . . . . . . . :      SocketInit
Statement . . . . . . . . . :      1279
 Message . . . . :      Error detected by Directory Services s
 Cause . . . . . :      The Directory Services server 009557/Q
   detected error 3420 (Address already in use.) attempting
   communications socket. Recovery . . . :   Display messa
   CPE3420 for additional information. The server may be re
   Operations Navigator or by using the STRTCPSVR SERVER(*
   the problem continues to occur, contact your service r
   Technical description . . . . . . . . :     Error 3420
   attempt to use a socket that is already in use.
     07/30/01   08:26:52   QGLDUTIL         QDIRSRV
From module . . . . . . . . :      GLDSLSOC
 From procedure . . . . . . :      SocketStart
Statement . . . . . . . . . :      1149
To module . . . . . . . . . :      GLDSLSOC
To procedure . . . . . . . :      SocketStart
Statement . . . . . . . . . :      1149
 Message . . . . :      Socket error for Directory S
 Cause . . . . . :      The Directory Services ser
   detected a socket initialization error for
   Restart the server using AS/400 Operations
```

Examine the output for information about the Directory Server. In this example, the server needs to be restarted.

B. Another problem may be the Administrator's password is incorrect. Be sure you use the correct upper or lower case when configuring the server's Administrator's password.

C. There may be no entries in the System Distribution Directory (SDD). A Technical Studio topic on adding users to the SDD can be found in *e-business 101* lesson 3, step 2.

Select a country

← Technical Studio Home

Configuring the OS/400 LDAP Server

· Verify these Pre-Configuration Tasks

· Configure and start the OS/400 LDAP server

· Publish to the LDAP directory from the OS/400 SDD

· Verify the connection to the OS/400 LDAP server

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

WRKRDBDIRE - Verify the local database entry.
The Work with Relational Database Directory Entries screen shows all of the entries in the relational database directory.

To verify a local entry:

1. From the iSeries Command line, type:

   WRKRDBDIRE

2. Press the **Enter** key. The *Work with Relational Database Directory Entries* screen appears:

```
                  Work with Relational Database Directory En

Position to  . . . . . .     _____

Type options, press Enter.
  1=Add    2=Change    4=Remove    5=Display details    6=P

            Relational            Remote
Option      Database              Location

  _         _____      
  _         SYS400_DB2            *LOCAL




F3=Exit    F5=Refresh    F6=Print list    F
```
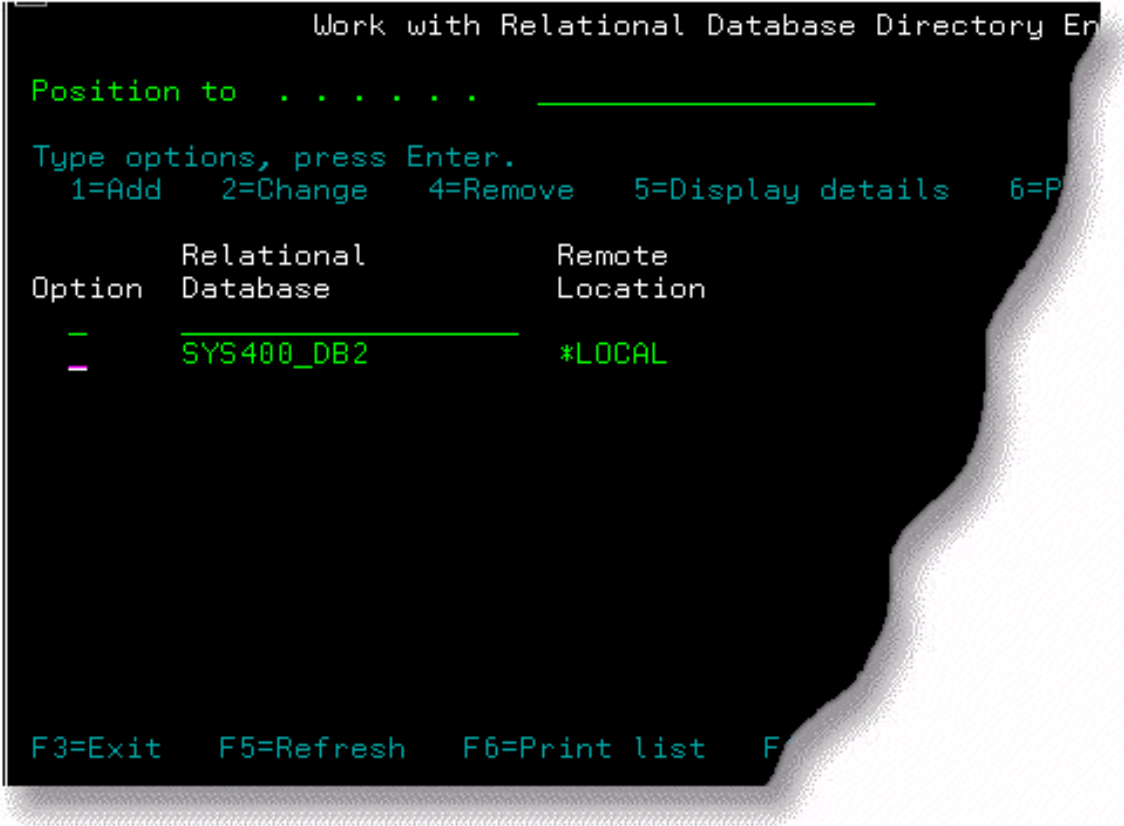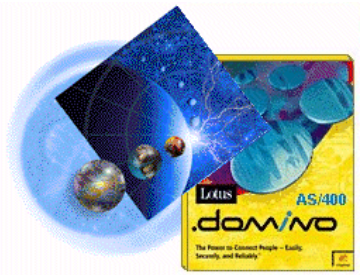
3. Record the **Relational Database** entry that is defined as ***LOCAL** under **Remote Location**. (In our example: SYS400_DB2) If you find that there are **no** *LOCAL entries, add an entry to identify this DB2/400 database.

Select a country

← Technical Studio Home

Configuring the OS/400 LDAP Server

- Verify these Pre-Configuration Tasks

- Configure and start the OS/400 LDAP server

- Publish to the LDAP directory from the OS/400 SDD

- Verify the connection to the OS/400 LDAP server

Related links:

iSeries 400 Directory Services (LDAP)

Redbook, LDAP Implementation Cookbook

Tech Studio e-business 101

IBM SecureWay Directory

Domino on Technical Studio Home Page

ITSO Redbooks

Domino for iSeries Home Page

Add a Local Database Entry
In order for LDAP to connect to a DB2/400 database, your iSeries Relational Database Entry needs to be defined. If you find that there are **no** *LOCAL entries, add an entry to identify this DB2/400 database.

Follow these few steps to add a Relational Database Entry.

1. On your iSeries command line, type:

   WRKRDBDIRE

   And press the **Enter** key.
   The *Work with Relational Database Directory Entries* screen appears.

2. Enter a **1** in the **Option** column and a name you wish to assign to this AS/400 DB2 database in the **Relational Database** column (e.g., SYS400).
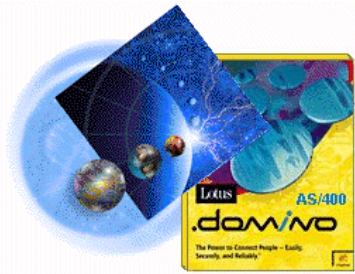
```
                       Work with Relational Database Directory Ent

   Position to  . . . . . .     _____

   Type options, press Enter.
     1=Add    2=Change    4=Remove    5=Display details    6=Pr

                 Relational            Remote
   Option        Database              Location
     1           SYS400_               

   F3=Exit    F5=Refresh    F6=Print list    F1
```

3. Enter ***LOCAL** on the **Remote Location Name or Address** line.

```
                        Add RDB Directory Entry (ADDRDBDIRE)

 Type choices, press Enter.

 Relational database  . . . . . . > SYS400           Charact
 Remote location:
   Name or address  . . . . . . .   *LOCAL_____

 _____
 _____

 _____
   Type . . . . . . . . . . . . .   ____           *SN
 Text . . . . . . . . . . . . . .   *BLANK_____
 _____

 F3=Exit   F4=Prompt   F5=Refresh   F12=Canc
 F24=More keys
```
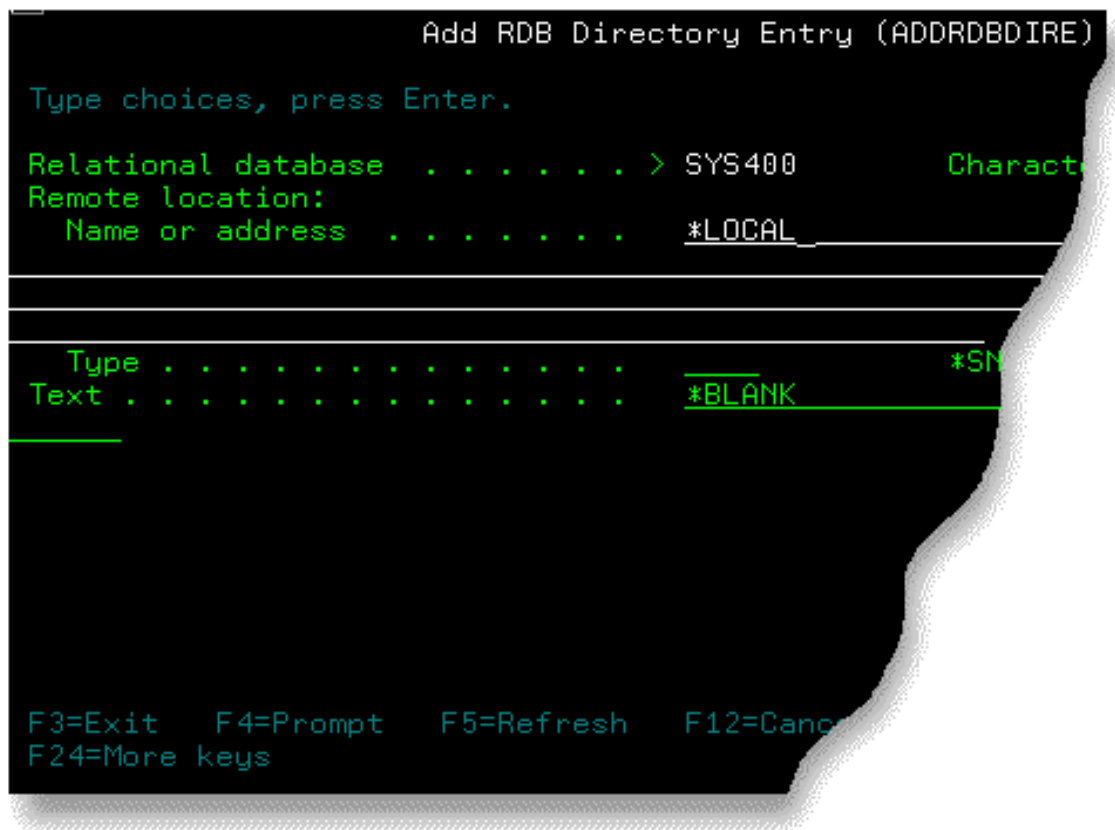
4. Press the **Enter** key to save and exit.

The *Relational Database Directory Entry* is used by the LDAP configuration portion of this workshop.

AS/400 Directory Services (LDAP)

What's New

IBM SecureWay Directory

Partners in Development

iSeries Online Library

iSeries Information Center

IBM Redbooks

Education

AS/400 Technical Support

Related links:

How to buy

Directory Services (LDAP):
Question and Answers

Overview Information

1. What is LDAP?
2. How do I get LDAP on my system and what does it cost?
3. Where do I find technical information on Directory Services (LDAP)?
4. What are the V4R4 changes to LDAP?
5. What are the V4R5 changes to LDAP?
6. LDAP FAQs from Partners in Development
7. Partners in Development web page

Installation and Configuration

1. How do I install an LDAP server on my system?
2. How do I change my LDAP server configuration?

Security

1. How is LDAP secured?
2. What is an Access Control List (ACL)?

Messages

1. Why do I get GLD0120 message in the servers job log even after a successful bind?

Publishing

1. How do I publish System Distribution Directory users to LDAP?
2. Checklist for ensuring you have publishing set up correctly for users
3. How do I publish OS/400 information to LDAP?

Overview information answers

1. **What is LDAP?**

   LDAP stands for 'Lightweight Directory Access Protocol'. In 1988, the CCITT (Consultative Committee on International Telephony and Telegraphy), created the X.500 standard, which became the ISO 9594, Data Communications Network Directory, Recommendations X.500-X.521 in 1990, though it is still commonly referred to as X.500. X.500 organizes directory entries in a hierarchical name space capable of supporting large amounts of information and specifies that communication between the directory client and the directory server uses the directory access protocol (DAP). However, as an application layer protocol, the DAP requires the entire OSI protocol stack to operate. Supporting the OSI protocol stack requires more resources than available in many small environments.

   Therefore, an interface to an X.500 directory server using a less resource-intensive or lightweight protocol was desired. LDAP was developed at the University of Michigan as a lightweight alternative to DAP (thus the name LDAP). LDAP requires the lighter weight and more popular TCP/IP protocol stack rather than the OSI protocol stack. LDAP also simplifies some X.500 operations and omits some esoteric features.

   LDAP defines a communication protocol. That is, it defines the transport and format of messages used by a client to access data in an X.500-like directory. LDAP does not define the directory service itself. However, when referring to a directory that can be accessed using LDAP, the directory is usually called an LDAP directory. Therefore, LDAP directories can be implemented in many different ways. IBM implements cross platform LDAP directories using DB2 and Lotus Domino.

   See **Overview** for more information on LDAP. Also see **Is LDAP your Directory Solution?**

2. **How do I get LDAP on my system and what does it cost?**

   Since V4R3, LDAP has been included free in OS/400 as part of Directory Services for OS/400 (option 32). Directory Services includes an LDAP server and complete set of LDAP clients and utilities.

   The LDAP server uses DB2/400 for storing the directory information and is configured using Operations Navigator.

   The OS/400 LDAP client supports accessing any LDAP server from all OS/400 ILE programming languages; C, COBOL and RPG. An LDAP client for Windows is included with OS/400 Client Access and a Java client is included in OS/400's support of Java Naming and Directory (JNDI).

   Command line utilities are provided for accessing an LDAP server from Windows and OS/400. These utilities are compatible with LDAP utilities provided for other operating systems and allow you to search, add, modify and delete directory information.

3. **Where do I find technical information on Directory Services (LDAP)?**

   The technical articles for Directory Services (LDAP) is found at Information Center. In 'Information Center' specify the release and language you want, expand 'Networking', then select 'Directory Services (LDAP)'.

4. **What are the V4R4 changes to LDAP?**

   See [V4R4 changes for LDAP](#).

5. **What are the V4R5 changes to LDAP?**

   See [V4R5 changes for LDAP](#).

Installation and Configuration answers

1. **How do I install an LDAP server on my system?**

   See [Configuring and Administering your LDAP server](#) for information on installing an LDAP server on your system.

   The [Information Center](#) has detailed articles on installing an LDAP server. In 'Information Center' specify the release and language you want, expand 'Networking', then select 'Directory Services (LDAP)'. Expand 'Getting Started with Directory Services'. Expand 'Installing and Configuring Directory Services'.

2. **How do I change my LDAP server configuration?**

   See [Configuring and Administering your LDAP server](#) for information on changing your LDAP server configuration.

   The [Information Center](#) has detailed articles on configuring your LDAP server. In 'Information Center' specify the release and language you want, expand 'Networking', then select 'Directory Services (LDAP)'. Expand 'Getting Started with Directory Services'. Expand 'Installing and Configuring Directory Services'.

Security answers

1. **How is LDAP secured?**

   To make communications with your LDAP directory server more secure, Directory Services can use Secure Sockets Layer (SSL) security. You can use SSL to communicate with LDAP clients, as well as with replica LDAP servers. SSL is the standard for Internet security. To use SSL, you must have Digital Certificate Manager (DCM), option 34 of OS/400, installed on your system. DCM provides an interface for you to create and manage digital certificates and key ring files.

   See [Information Center](#) for information on SSL. In 'Information Center' specify the release and language you want, expand 'Networking', then select 'Directory Services (LDAP)'. Expand 'Directory Services concepts and reference information' and then expand 'Managing ownership and access of directory data'.

2. **What is an Access Control List (ACL)?**

   An Access Control List (ACL) allows you to manage who can access directory information in your network directory. In many cases, you probably would not want to restrict access to data on your LDAP directory server. For example, an LDAP server on your company Intranet might contain a telephone directory of company employees. You would probably want all employees to be able to view the data in this directory. Imagine, however, that the president of your company does not want all employees to be able to access her telephone number. In that case, you could create an access control list (ACL). With this ACL, you could restrict access to her server entry to only those employees the president wanted to receive calls from.

   See [Configuring and Administering your LDAP server](#) for information on ACLs.

   The [Information Center](#) has detailed articles on ACLs. In 'Information Center' specify the release and language you want, expand 'Networking', then select 'Directory Services (LDAP)'. Expand 'Administering the LDAP directory server' and then expand 'Managing ownership and access of directory data'. You can also find ACL information when you expand 'Directory Services concepts and reference information' and then expand 'Managing ownership and access of directory data'.

Message answers

1. **Why do I get GLD0120 message in the servers job log even after a successful bind?**

   This message will be logged in the servers job log for several reasons. If a bind is requested but the dn does not exist on the server, or the if the dn exists but the password is incorrect, then GLD0120 will be logged. The GLD0120 message can also be logged if a version 3 (V3) enabled client tries to first connect as V3, then as version 2 (V2). The V2 bind is successful, but the V3 bind was not because the server does not support V3 in V4R3 and V4R4.

Publishing answers

1. **How do I publish System Distribution Directory users to LDAP?**

   In V4R3 and later, you can now publish users from the system distribution directory to an LDAP server and keep the LDAP directory synchronized with changes made in the system distribution directory. You can then use the information that you publish in LDAP from applications like the Netscape Messenger Mailbox using the 'Search directory' function or from other LDAP applications that access address book information.

   See [Publishing AS/400 System Distribution Directory to LDAP](#) for an article published in AS/400 Magazine on how to publish users to LDAP.

   For more information, see [Information Center](#) - in 'Information Center' specify the release and language you want, expand 'Networking', then select 'Directory Services (LDAP)'. Expand 'Administering the LDAP directory server', 'Moving LDAP directory data between systems' and then 'Publishing user information to the directory server'.

   Also, see [QGLDSSDD API](#) - in 'Online Library' specify the language you want, select the release, search all books and input 'System API Reference', select 'Part 2. Application Programming Interfaces (APIs)', 'OS/400 Directory Services APIs', and then 'Synchronize System Distribution Directory to LDAP (QGLDSSDD) API'.

2. **Checklist for ensuring you have publishing set up correctly for users**

See How do I publish System Distribution Directory users to LDAP?.

Also you can do the following to verify you have everything set up correctly.

1. Is TCP/IP configured on your system? From the command line, enter CHGTCPDMN and press F4. Ensure the host and domain name are set. From the command line, enter CHGSMTPA and press F4. Verify the user ID delimiter and press the 'Enter' key. If the ldap server is on OS/400, can you ping the system? If not, you may not have your domain name server or your host table set up correctly. If you have a long TCP/IP name in your host table (CFGTCP option 10) you may want to try the short name.

2. Do you have an ldap server configured? Publishing can be done to an ldap server on an OS/400 or to other IBM platform ldap servers. Ensure you know the administrator dn and password that you used to configure the ldap server. See Configuring and Administering your LDAP server for information on installing an LDAP server on your system.

3. Is the ldap server active? If the ldap server is on OS/400, you can check this by using the command WRKACTJOB SBS(QSYSWRK) and if the job QDIRSRV is listed in SELW status, then the ldap server is active and ready for requests.

4. On your PC that you have Operations Navigator for OS/400, can you ping the system the LDAP server is on? If not, you need to update the TCP/IP Hosts file (see Windows help for "HOSTS file").

5. Did you configure the 'Directory Services' property of the system in Operations Navigator that you are publishing users on? If not, you need to use Operations Navigator, select the system and right click to get 'properties'. Select the 'Directory Services' tab. For V4R4 and later, select 'Users' and then press 'Configure' button. Fill in the information. Ensure the name of the server is an IP name and not the hardcoded IP address.

6. Did you press the 'Verify' button on the 'Directory Services' property page and did you input the ldap administrator dn and password or another user that you have given administrator authorization to? For example, the default ldap administrator dn is 'cn=administrator'. The administrator dn was specified when you set up your ldap server. Did you get a successful confirmation back from the 'Verify' button? This does two things for you - one, it verifies that the dn and password that you input is valid; and two, it creates an entry on the ldap server for the publishing of users if it does not exist (if you responded 'Yes' to the question 'Directory path does not exist. Would you like to create it?').

7. If you get the error 'xxx could not be created. Enter a different path or create the path manually in your directory' this indicates either the suffix does not exist on the server or directory data for the parent dn does not exist.

   If you are not publishing directly to one of the suffixes you specified on the ldap server, does your ldap server have directory data for the suffix that you want to publish to? For example, if you set up a suffix of 'o=DeltaCorp,c=US', but you want to publish to 'cn=users,o=DeltaCorp,c=US', do you have the directory data for the 'o=DeltaCorp,c=US' suffix on the server (also called the parent dn)? To create the parent dn data, you can specify the suffix data (ie o=DeltaCorp,c=US) and press the 'Verify' button. This will create the parent dn. You can then specify the directory path below this parent dn (ie cn=users,o=DeltaCorp,c=US) and press the 'Verify' button again.

8. When attempting to publish to the LDAP server and you are getting GLD0301 message with return code 53, you probably have the property value for the Directory Services server 'Allow directory updates' unchecked. From Operations Navigator, Directory Services properties on the 'General' page, ensure the box for 'Allow directory updates' is checked.

9. For V4R3: Did you call the QGLDSSDD api correctly? The correct call is "CALL PGM(QDIRSRV/QGLDSSDD) PARM(*ALL 'LDAPuserid' 'LDAPpassword' 'SSLkeyring' 'SSLpassword' 0)" for the first call and "CALL PGM(QDIRSRV/QGLDSSDD) PARM(*CHG 'LDAPuserid' 'LDAPpassword' 'SSLkeyring' 'SSLpassword' 0)" for any changes from the SDD to be applied. The 'LDAPuserid' should be the same dn that you input in the 'Verify' step above because that user and password has been verified. If you do not have SSL, specify '0' for those parameters. Also, ensure you specify single quotes as the example shows.

   So for example, "CALL PGM(QDIRSRV/QGLDSSDD) PARM(*ALL 'cn=administrator' 'secretpassword' 0 0 0)" is a valid call if you do not need SSL.

   In V4R4 and later, the call to the QGLDSSDD api is done automatically when you configure publishing for users.

10. If you are not successful in publishing users, check errors from the ldap server. If the ldap server is on OS/400, you can do this using WRKACTJOB SBS(QSYSWRK) and specify option 5 for the QDIRSRV job listed.

---

3. **How do I publish OS/400 information to LDAP?**

You can configure your system to publish certain OS/400 information into an LDAP directory server on the same OS/400 or on a different OS/400. This information will then automatically be published to the LDAP directory server when this information is changed on the OS/400 system.

In V4R4 and later, you can publish information about computers on your network. Additionally, you can incorporate publishing to the LDAP directory server into your own programs to publish other types of information.

See Information Center for information on publishing. In 'Information Center' specify the release and language you want, expand 'Networking', then select 'Directory Services (LDAP)'. Expand 'Administering the LDAP directory server' and then expand 'Moving LDAP directory data between systems'. This information will be available at V4R4 GA.